Quantum Information and Computation, Vol. 0, No. 0 (2003) 000–000
© Rinton Press

COMPUTATIONAL COMPLEXITY OF THE QUANTUM SEPARABILITY PROBLEM

LAWRENCE M. IOANNOU
*Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Wilberforce Road
Cambridge, Cambridgeshire, CB3 0WA, United Kingdom*

Received (received date)
Revised (revised date)

Ever since entanglement was identified as a computational and cryptographic resource, researchers have sought efficient ways to tell whether a given density matrix represents an unentangled, or *separable*, state. This paper gives the first systematic and comprehensive treatment of this (bipartite) quantum separability problem, focusing on its deterministic (as opposed to randomized) computational complexity. First, I review the one-sided tests for separability, paying particular attention to the semidefinite programming methods. Then, I discuss various ways of formulating the quantum separability problem, from exact to approximate formulations, the latter of which are the paper's main focus. I then give a thorough treatment of the problem's relationship with the complexity classes NP, NP-complete, and co-NP. I also discuss extensions of Gurvits' NP-hardness result to strong NP-hardness of certain related problems. A major open question is whether the NP-contained formulation (QSEP) of the quantum separability problem is Karp-NP-complete; QSEP may be the first natural example of a problem that is Turing-NP-complete but not Karp-NP-complete. Finally, I survey all the proposed (deterministic) algorithms for the quantum separability problem, including the bounded search for symmetric extensions (via semidefinite programming), based on the recent quantum de Finetti theorem [1, 2, 3]; and the entanglement-witness search (via interior-point algorithms and global optimization) [4, 5]. These two algorithms have the lowest complexity, with the latter being the best under advice of asymptotically optimal point-coverings of the sphere.

Keywords: The contents of the keywords
Communicated by: to be filled by the Editorial

1 Introduction

If a d-dimensional quantum physical system can be physically partitioned into two subsystems (denoted by superscripts A and B) of dimensions M and N, such that $d = MN$, then the pure state $|\psi\rangle$ of this total system may be *separable*, which means $|\psi\rangle = |\psi^{\mathrm{A}}\rangle \otimes |\psi^{\mathrm{B}}\rangle$, for $|\psi^{\mathrm{A}}\rangle \in \mathbf{C}^M$ and $|\psi^{\mathrm{B}}\rangle \in \mathbf{C}^N$ and where "$\otimes$" denotes the Kronecker (tensor) product. Without loss of generality, assume $M \leq N$ (except in Section 2.2.5). If $|\psi\rangle$ is not separable, then it is *entangled* (with respect to that particular partition).

Denote by $\mathcal{D}(V)$ the set of all density operators mapping complex vector space V to itself; let $\mathcal{D}_{M,N} := \mathcal{D}(\mathbf{C}^M \otimes \mathbf{C}^N)$. The *maximally mixed state* is $I_{M,N} := I/MN$, where I denotes the identity operator. A pure state $|\psi\rangle$ is separable if and only if $\mathrm{tr}_{\mathrm{B}}(|\psi\rangle\langle\psi|)$ is a pure state, where "tr_{B}" denotes the partial trace with respect to subsystem B; a pure state is called *maximally entangled* if $\mathrm{tr}_{\mathrm{B}}(|\psi\rangle\langle\psi|)$ is the maximally mixed state I/M in the space of density operators on the A-subsystem $\mathcal{D}(\mathbf{C}^M)$. Thus, the mixedness of $\mathrm{tr}_{\mathrm{B}}(|\psi\rangle\langle\psi|)$ is some "measure" of the entanglement of $|\psi\rangle$.

A mixed state $\rho \in \mathcal{D}_{M,N}$ is *separable* if and only if it may be written $\rho = \sum_{i=1}^{k} p_i \rho_i^{\mathrm{A}} \otimes \rho_i^{\mathrm{B}}$ with $p_i \geq 0$ and $\sum_i p_i = 1$, and where $\rho_i^{\mathrm{A}} \in \mathcal{D}(\mathbf{C}^M)$ is a (mixed or pure) state of the A-subsystem (and similarly for $\rho_i^{\mathrm{B}} \in \mathcal{D}(\mathbf{C}^N)$); when $k = 1$, ρ is a *product state*. Let $\mathcal{S}_{M,N} \subset \mathcal{D}_{M,N}$ denote the separable states; let $\mathcal{E}_{M,N} := \mathcal{D}_{M,N} \setminus \mathcal{S}_{M,N}$ denote the entangled states. The following fact will be used several times throughout this work:

Fact 1 ([6]) *If $\sigma \in \mathcal{S}_{M,N}$, then σ may be written as a convex combination of M^2N^2 pure product states, that is,*

$$\sigma = \sum_{i=1}^{M^2N^2} p_i |\psi_i^{\mathrm{A}}\rangle\langle\psi_i^{\mathrm{A}}| \otimes |\psi_i^{\mathrm{B}}\rangle\langle\psi_i^{\mathrm{B}}|, \tag{1}$$

where $\sum_{i=1}^{M^2N^2} p_i = 1$ and $0 \leq p_i \leq 1$ for all $i = 1, 2, \ldots, M^2N^2$.

Recall that a set of points $\{x_1, \ldots, x_j\} \subset \mathbf{R}^n$ is *affinely independent* if and only if the set $\{x_2 - x_1, x_3 - x_1, \ldots, x_j - x_1\}$ is linearly independent in $\mathbf{R}^n$. Recall also that the *dimension* of $X \subset \mathbf{R}^n$ is defined as the size of the largest affinely-independent subset of X minus 1. Fact 1 is based on the well-known theorem of Carathéodory that any point in a compact convex set $X \subset \mathbf{R}^n$ of dimension k can be written as a convex combination of $k+1$ affinely-independent extreme points of X.

Definition 1 (Formal quantum separability problem) *Let $\rho \in \mathcal{D}_{M,N}$ be a mixed state. Given the matrix*[a] *$[\rho]$ (with respect to the standard basis of $\mathbf{C}^M \otimes \mathbf{C}^N$) representing ρ, decide whether ρ is separable.*

1.1 One-sided tests and restrictions

Shortly after the importance of the quantum separability problem was recognized in the quantum information community, efforts were made to solve it reasonably efficiently. In this vein, many one-sided tests have been discovered. A *one-sided test (for separability)* is a computational procedure (with input $[\rho]$) whose output can only ever imply *one* of the following (with certainty):

- ρ is entangled (in the case of a *necessary test*)
- ρ is separable (in the case of a *sufficient test*).

There have been many good articles (e.g. [7, 8, 9]) which review the one-sided (necessary) tests. As this work is concerned with algorithms that are both necessary and sufficient tests for separability for all M and N – and whose computer-implementations have a hope of being useful in low dimensions – I only review in detail the one-sided tests which give rise to such

[a] We do not yet define how the entries of this matrix are encoded; at this point, we assume all entries have some finite representation (e.g. "$\sqrt{2}$") and that the computations on this matrix can be done exactly.

algorithms (see Section 1.2). But here is a list of popular conditions on ρ giving rise to efficient one-sided tests for finite-dimensional bipartite separability:

Necessary conditions for ρ to be separable

- PPT test [10]: $\rho^{T_{\rm B}} \geq 0$, where "$T_{\rm B}$" denotes partial transposition
- Reduction criterion [11]: $\rho^{\rm A} \otimes I - \rho \geq 0$ and $I \otimes \rho^{\rm B} - \rho \geq 0$, where $\rho_{\rm A} := {\rm tr}_{\rm B}(\rho)$ and "${\rm tr}_{\rm B}$" denotes partial trace (and similarly for $\rho_{\rm B}$)
- Entropic criterion for $\alpha = 2$ and in the limit $\alpha \rightarrow 1$ [12]: $S_\alpha(\rho) \geq \max\{S_\alpha(\rho_{\rm A}), S_\alpha(\rho_{\rm B})\}$; where, for $\alpha > 1$, $S_\alpha(\rho) := \frac{1}{1-\alpha}\ln({\rm tr}(\rho^\alpha))$
- Majorization criterion [13]: $\lambda^{\downarrow}_{\rho} \prec \lambda^{\downarrow}_{\rho^{\rm A}}$ and $\lambda^{\downarrow}_{\rho} \prec \lambda^{\downarrow}_{\rho^{\rm B}}$, where $\lambda^{\downarrow}_{\tau}$ is the list of eigenvalues of τ in nonincreasing order (padded with zeros if necessary), and $x \prec y$ for two lists of size s if and only if the sum of the first k elements of list x is less than or equal to that of list y for $k = 1, 2, ..., s$; the majorization condition implies $\max\{{\rm rank}(\rho^{\rm A}), {\rm rank}(\rho^{\rm B})\} \leq {\rm rank}(\rho)$.
- Computable cross-norm/reshuffling criterion [14, 15]: $||\mathcal{U}(\rho)||_1 \leq 1$, where $||X||_1 := {\rm tr}(\sqrt{X^\dagger X})$ is the trace norm; and $\mathcal{U}(\rho)$, an $M^2 \times N^2$ matrix, is defined on product states as $\mathcal{U}(A \otimes B) := v(A)v(B)^T$, where, relative to a fixed basis, $[v(A)] = ({\rm col}_1([A])^T, \ldots, {\rm col}_M([A])^T)^T$ (and similarly for $v(B)$), where ${\rm col}_i([A])$ is the ith column of matrix $[A]$; more generally [16], any linear map $\mathcal{U}$ that does not increase the trace norm of product states may be used.

Sufficient conditions for ρ to be separable

- Distance from maximally mixed state (see also [17]):
  - [18]: e.g. ${\rm tr}(\rho - I_{M,N})^2 \leq 1/MN(MN-1)$
  - [19, 20] $\lambda_{\min}(\rho) \geq (2 + MN)^{-1}$, where $\lambda_{\min}(\rho)$ denotes the smallest eigenvalue of ρ
- When $M = 2$ [21]: $\rho = \rho^{T_A}$.

When ρ is of a particular form, the PPT test is necessary and sufficient for separability. This happens when

- $MN \leq 6$ [22]; or
- ${\rm rank}(\rho) \leq N$ [21, 23], see also [24].

The criteria not based on eigenvalues are obviously efficiently computable; i.e. computing the natural logarithm can be done with a truncated Taylor series, and the rank can be computed by Gaussian elimination. That the tests based on the remaining criteria are efficiently computable follows from the efficiency of algorithms for calculating the spectrum of a Hermitian operator. The method of choice for computing the entire spectra is the QR algorithm (see any of [25, 26, 27]), which has been shown to have good convergence properties [28].

In a series of articles ([29], [21], [23]), various conditions for separability were obtained which involve product vectors in the ranges of ρ and ρ^{T_A}. Any constructive separability checks given therein involve computing these product vectors, but no general bounds were obtained by the authors on the complexity of such computations.

1.2 One-sided tests based on semidefinite programming

Let $\mathbf{H}_{M,N}$ denote the set of all Hermitian operators mapping $\mathbf{C}^M \otimes \mathbf{C}^N$ to $\mathbf{C}^M \otimes \mathbf{C}^N$; thus, $\mathcal{D}_{M,N} \subset \mathbf{H}_{M,N}$. This vector space is endowed with the Hilbert-Schmidt inner product $\langle X, Y \rangle \equiv \mathrm{tr}(AB)$, which induces the corresponding norm $||X|| \equiv \sqrt{\mathrm{tr}(X^2)}$ and distance measure $||X - Y||$. By fixing an orthogonal Hermitian basis for $\mathbf{H}_{M,N}$, the elements of $\mathbf{H}_{M,N}$ are in one-to-one correspondence with the elements of the real Euclidean space $\mathbf{R}^{M^2N^2}$. If the Hermitian basis is orthonormal, then the Hilbert-Schmidt inner product in $\mathbf{H}_{M,N}$ corresponds exactly to the Euclidean dot product in $\mathbf{R}^{M^2N^2}$.

Let us be more precise. Let $\mathcal{B} = \{X_i : i = 0, 1, \ldots, M^2N^2 - 1\}$ be an orthonormal, Hermitian basis for $\mathbf{H}_{M,N}$, where $X_0 \equiv \frac{1}{\sqrt{MN}} I$. For concreteness, we can assume that the elements of $\mathcal{B}$ are tensor-products of the (suitably normalized) canonical generators of SU(M) and SU(N), given e.g. in [30]. Note $\mathrm{tr}(X_i) = 0$ for all $i > 0$. Define $v : \mathbf{H}_{M,N} \to \mathbf{R}^{M^2N^2-1}$ as

$$v(A) := \begin{bmatrix} \mathrm{tr}(X_1 A) \\ \mathrm{tr}(X_2 A) \\ \vdots \\ \mathrm{tr}(X_{M^2N^2-1} A) \end{bmatrix}. \tag{2}$$

Via the mapping v, the set of separable states $\mathcal{S}_{M,N}$ can be viewed as a full-dimensional convex subset of $\mathbf{R}^{M^2N^2-1}$

$$\{v(\sigma) \in \mathbf{R}^{M^2N^2-1} : \sigma \in \mathcal{S}_{M,N}\}, \tag{3}$$

which properly contains the origin $v(I_{M,N}) = \overline{0} \in \mathbf{R}^{M^2N^2-1}$ (recall that there is a ball of separable states of nonzero radius centred at the maximally mixed state $I_{M,N}$).

Thus $\mathcal{D}_{M,N}$ and $\mathcal{S}_{M,N}$ may be viewed as subsets of the Euclidean space $\mathbf{R}^{M^2N^2}$; actually, because all density operators have unit trace, $\mathcal{D}_{M,N}$ and $\mathcal{S}_{M,N}$ are full-dimensional subsets of $\mathbf{R}^{M^2N^2-1}$. This observation aids in solving the quantum separability problem, allowing us to apply easily well-studied mathematical-programming tools. The following is from the popular review article of semidefinite programming in [31].

Definition 2 (Semidefinite program (SDP)) *Given the vector $c \in \mathbf{R}^m$ and Hermitian matrices $F_i \in \mathbf{C}^{n\times n}$, $i = 0, 1, \ldots, m$,*

$$\begin{aligned} &\textit{minimize} && c^T x && (4)\\ &\textit{subject to:} && F(x) \geq 0, && (5) \end{aligned}$$

where $F(x) := F_0 + \sum_{i=1}^m x_i F_i$.

Call x *feasible* when $F(x) \geq 0$. When $c = 0$, the SDP reduces to the *semidefinite feasibility problem*, which is to find an x such that $F(x) \geq 0$ or assert that no such x exists. Semidefinite programs can be solved efficiently, in time $O(m^2 n^{2.5})$. Most algorithms are iterative. Each iteration can be performed in time $O(m^2 n^2)$. The number of required iterations has an analytical bound of $O(\sqrt{n})$, but in practice is more like $O(\log(n))$ or constant.

1.2.1 A test based on symmetric extensions

Consider a separable state $\sigma = \sum_i p_i |\psi_i^{\mathrm{A}}\rangle\langle\psi_i^{\mathrm{A}}| \otimes |\psi_i^{\mathrm{B}}\rangle\langle\psi_i^{\mathrm{B}}|$, and consider the following *symmetric extension of* σ *to* k *copies of subsystem* A ($k \geq 2$):

$$\tilde{\sigma}_k = \sum_i p_i (|\psi_i^{\mathrm{A}}\rangle\langle\psi_i^{\mathrm{A}}|)^{\otimes k} \otimes |\psi_i^{\mathrm{B}}\rangle\langle\psi_i^{\mathrm{B}}|. \tag{6}$$

The state $\tilde{\sigma}_k$ is so called because it satisfies two properties: (i) it is symmetric (unchanged) under permutations (swaps) of any two copies of subsystem A; and (ii) it is an extension of σ in that tracing out any of its $(k-1)$ copies of subsystem A gives back σ. For an arbitrary density operator $\rho \in \mathcal{D}(\mathbf{C}^M \otimes \mathbf{C}^N)$, define a *symmetric extension of* ρ *to* k *copies of subsystem* A as any density operator $\rho' \in \mathcal{D}((\mathbf{C}^M)^{\otimes k} \otimes \mathbf{C}^N)$ that satisfies (i) and (ii) with ρ in place of σ. If ρ does not have a symmetric extension to k_0 copies of subsystem A for some k_0, then $\rho \notin \mathcal{S}_{M,N}$ (else we could construct $\tilde{\rho}_{k_0}$). Thus a method for searching for symmetric extensions of ρ to k copies of subsystem A gives a sufficient test for separability.

Doherty et al. [1, 2] showed that the search for a symmetric extension to k copies of ρ (for any fixed k) can be phrased as a SDP. This result, combined with the "quantum de Finetti theorem" [32, 33] that $\rho \in \mathcal{S}_{M,N}$ if and only if, for all k, ρ has a symmetric extension to k copies of subsystem A, gives an infinite hierarchy (indexed by $k = 2, 3, \ldots$) of SDPs with the property that, for each entangled state ρ, there exists a SDP in the hierarchy whose solution will imply that ρ is entangled.

Actually, Doherty et al. develop a stronger test, inspired by Peres' PPT test. The state $\tilde{\sigma}_k$, which is positive semidefinite, satisfies a third property: (iii) it remains positive semidefinite under all possible partial transpositions. Thus $\tilde{\sigma}_k$ is more precisely called a *PPT symmetric extension*. The SDP can be easily modified to perform a search for PPT symmetric extensions without any significant increase in computational complexity (one just needs to add constraints that force the partial transpositions to be positive semidefinite). This strengthens the separability test, because a given (entangled) state ρ may have a symmetric extension to k_0 copies of subsystem A but may not have a PPT symmetric extension to k_0 copies of subsystem A (Doherty et al. also show that the $(k+1)$st test in this stronger hierarchy subsumes the kth test).

The final SDP has the following form:

$$\begin{array}{lrcl} \text{minimize} & 0 & & \\ \text{subject to:} & \tilde{X}_k & \geq & 0 \\ & (\tilde{X}_k)^{T_j} & \geq & 0, \quad j \in J, \end{array} \tag{7}$$

where $\tilde{X}_k$ is a parametrization of a symmetric extension of ρ to k copies of subsystem A, and J is the set of all subsets of the $(k+1)$ subsystems that give rise to inequivalent partial transposes $(\tilde{X}_k)^{T_j}$ of $\tilde{X}_k$. By noting that we can restrict our search to so-called *Bose-symmetric extensions*, where $(I \otimes P)\rho' = \rho'$ for all $k!$ permutations P of the k copies of subsystem A (as opposed to just extensions where $(I \otimes P)\rho'(I \otimes P^\dagger) = \rho'$ for all permutations P), the number of variables of the SDP is $m = ((d_{S_k})^2 - M^2)N^2$, where $d_{S_k}= \binom{M+k-1}{k}$ is the dimension of the symmetric subspace of $(\mathbf{C}^M)^{\otimes k}$. The size of the matrix $\tilde{X}_k$ for the first constraint is $(d_{S_k})^2N^2$. The number of inequivalent partial transpositions is $|J| = k$.[b] The constraint corresponding to the transposition of l copies of A, $l = 1, 2, ..., k-1$, has a matrix of size $(d_{S_l})^2(d_{S_{(k-l)}})^2N^2$ [2]. I will estimate the total complexity of this approach to the quantum separability problem in Section 3.2.

1.2.2 A test based on semidefinite relaxations

Doherty et al. formulate a *hierarchy of necessary criteria* for separability in terms of semidefinite programming – each separability criterion in the hierarchy may be checked by a SDP. As it stands, their approach is manifestly a one-sided test for separability, in that at no point in the hierarchy can one conclude that the given $[\rho]$ corresponds to a separable state (happily, recent results show that, for sufficiently large k, the symmetric-extension test is a complete approximate separability test; see Section 3.2).

Eisert et al. [34] formulate a *necessary and sufficient criterion* for separability as a hierarchy of SDPs. Define the function

$$E_{d_2^2}(\rho) := \min_{x \in \mathcal{S}_{M,N}} \operatorname{tr}((\rho - x)^2) \tag{8}$$

for $\rho \in \mathcal{D}_{M,N}$. As $\operatorname{tr}((\rho - x)^2)$ is the square of the Euclidean distance from ρ to x, ρ is separable if and only if $E_{d_2^2}(\rho) = 0$. The problem of computing $E_{d_2^2}(\rho)$ (to check whether it is zero) is already formulated as a constrained optimization. The following observation helps to rewrite these constraints as low-degree polynomials in the variables of the problem:

Fact 2 ([34]) *Let O be a Hermitian operator and let $\alpha \in \mathbf{R}$ satisfy $0 < \alpha \leq 1$. If $tr(O^2) = \alpha^2$ and $tr(O^3) = \alpha^3$, then $tr(O) = \alpha$ and $rank(O) = 1$ (i.e. O corresponds to an unnormalized pure state).*

Combining Fact 2 with Fact 1, the problem is equivalent to

$$\begin{array}{lrcl}
\text{minimize} & \operatorname{tr}((\rho - \sum_{i=1}^{M^2N^2} X_i)^2) & & \\
\text{subject to:} & \operatorname{tr}(\sum_{i=1}^{M^2N^2} X_i) & = & 1 \\
& \operatorname{tr}((\operatorname{tr}_j(X_i))^2) & = & (\operatorname{tr}(X_i))^2, \\
& & & \text{for } i = 1, 2, \ldots, M^2N^2 \text{ and } j \in \{\text{A}, \text{B}\} \\
& \operatorname{tr}((\operatorname{tr}_j(X_i))^3) & = & (\operatorname{tr}(X_i))^3, \\
& & & \text{for } i = 1, 2, \ldots, M^2N^2 \text{ and } j \in \{\text{A}, \text{B}\},
\end{array} \tag{9}$$

where the new variables are Hermitian matrices X_i for $i = 1, 2, \ldots, M^2N^2$. The constraints do *not* require X_i to be tensor products of *unit-trace* pure density operators, because the positive coefficients (probabilities summing to 1) that would normally appear in the expression $\sum_{i=1}^{M^2N^2} X_i$ are absorbed into the X_i, in order to have fewer variables (i.e. the X_i are constrained to be density operators corresponding to unnormalized pure product states). Once

[b] Choices are: transpose subsystem B, transpose 1 copy of subsystem A, transpose 2 copies of subsystem A, ..., transpose $k-1$ copies of subsystem A. Transposing all k copies of subsystem A is equivalent to transposing subsystem B. Transposing with respect to both subsystem B and l copies of subsystem A is equivalent to transposing with respect to $k-l$ copies of subsystem A.

an appropriate Hermitian basis is chosen for $\mathbf{H}_{M,N}$, the matrices X_i can be parametrized by the real coefficients with respect to the basis; these coefficients form the real variables of the feasibility problem. The constraints in (9) are polynomials in these variables of degree less than or equal to 3.[c]

Polynomially-constrained optimization problems can be approximated by, or *relaxed* to, semidefinite programs, via a number of different approaches (see references in [34]).[d] Some approaches even give an asymptotically complete hierarchy of SDPs, indexed on, say, $i = 1, 2, \ldots$. The SDP at level $i+1$ in the hierarchy gives a better approximation to the original problem than the SDP at level i; but, as expected, the size of the SDPs grows with i so that better approximations are more costly to compute. The hierarchy is asymptotically complete because, under certain conditions, the optimal values of the relaxations converge to the optimal value of the original problem as $i \to \infty$. Of these approaches, the method of Lasserre [35] is appealing because a computational package [36] written in MATLAB is freely available. Moreover, this package has built into it a method for recognizing when the optimal solution to the original problem has been found (see [36] and references therein). Because of this feature, the one-sided test becomes, in practice, a full algorithm for the quantum separability problem. However, no analytical worst-case upper bounds on the running time of the algorithm for arbitrary $\rho \in \mathcal{D}_{M,N}$ are presently available.

1.2.3 Entanglement Measures

The function $E_{d_2^2}(\rho)$ defined in (8), but first defined in [37], is also known as an *entanglement measure*, which, at the very least, is a nonnegative real function defined on $\mathcal{D}_{M,N}$ (for a comprehensive review of entanglement measures, see [38]). If an entanglement measure $E(\rho)$ satisfies

$$E(\rho) = 0 \quad \Leftrightarrow \quad \rho \in \mathcal{S}_{M,N}, \tag{11}$$

then, in principle, any algorithm for computing $E(\rho)$ gives an algorithm for the quantum separability problem. Note that most entanglement measures E do not satisfy (11); most just satisfy $E(\rho) = 0 \Leftarrow \rho \in \mathcal{S}_{M,N}$.

[c] Alternatively, we could parametrize the pure states (composing X_i) in $\mathbf{C}^M$ and $\mathbf{C}^N$ by the real and imaginary parts of rectangularly-represented complex coefficients with respect to the standard bases of $\mathbf{C}^M$ and $\mathbf{C}^N$:

$$\begin{array}{lrcl} \text{minimize} & & 0 & \\ \text{subject to:} & \mathrm{tr}((\rho - \sum_{i=1}^{M^2N^2} |\psi_i^{\mathrm{A}}\rangle\langle\psi_i^{\mathrm{A}}| \otimes |\psi_i^{\mathrm{B}}\rangle\langle\psi_i^{\mathrm{B}}|)^2) & = & 0 \\ & \mathrm{tr}\left(\sum_{i=1}^{M^2N^2} |\psi_i^{\mathrm{A}}\rangle\langle\psi_i^{\mathrm{A}}| \otimes |\psi_i^{\mathrm{B}}\rangle\langle\psi_i^{\mathrm{B}}|\right) & = & 1. \end{array} \tag{10}$$

This parametrization hard-wires the constraint that the $|\psi_i^{\mathrm{A}}\rangle\langle\psi_i^{\mathrm{A}}|\otimes|\psi_i^{\mathrm{B}}\rangle\langle\psi_i^{\mathrm{B}}|$ are (unnormalized) pure product states, but increases the degree of the polynomials in the constraint to 4 (for the unit trace constraint) and 8 (for the distance constraint).

[d] For our purposes, the idea of a relaxation can be briefly described as follows. The given problem is to solve $\min_{x\in\mathbf{R}^n}\{p(x) : \; g_k(x) \geq 0, k = 1, \ldots, m\}$, where $p(x), g_i(x) : \; \mathbf{R}^n \to \mathbf{R}$ are real-valued polynomials in $\mathbf{R}[x_1, \ldots, x_n]$. By introducing new variables corresponding to products of the given variables (the number of these new variables depends on the maximum degree of the polynomials p, g_i), we can make the objective function linear in the new variables; for example, when $n = 2$ and the maximum degree is 3, if $p(x) = 3x_1 + 2x_1x_2 + 4x_1x_2^2$ then the objective function is c^Ty with $c = (0, 3, 0, 0, 2, 0, 0, 0, 4, 0) \in \mathbf{R}^{10}$ and $y \in \mathbf{R}^{10}$, where 10 is the total number of monomials in $\mathbf{R}[x_1, x_2]$ of degree less than or equal to 3. Each polynomial defining the feasible set $G := \{x \in \mathbf{R}^n : \; g_k(x) \geq 0, k = 1, \ldots, m\}$ can be viewed similarly. A relaxation of the original problem is a SDP with objective function c^Ty and with a (convex) feasible region (in a higher-dimensional space) whose projection onto the original space $\mathbf{R}^n$ approximates G. Better approximations to G can be obtained by going to higher dimensions.

A class of entanglement measures that do satisfy (11) are the so-called "distance measures" $E_d(\rho) := \min_{\sigma \in \mathcal{S}_{M,N}} d(\rho, \sigma)$, for any reasonable measure of "distance" $d(x, y)$ satisfying $d(x, y) \geq 0$ and $(d(x, y) = 0) \Leftrightarrow (x = y)$. If d is the square of the Euclidean distance, we get $E_{d_2^2}(\rho)$. Another "distance measure" is the von Neumann relative entropy $S(x, y) := \mathrm{tr}(x(\log x - \log y))$.

In Eisert et al.'s approach, we could replace $E_{d_2^2}$ by E_d for any "distance function" $d(\rho, \sigma)$ that is expressible as a polynomial in the variables of σ. What dominates the running time of Eisert et al.'s approach is the implicit minimization over $\mathcal{S}_{M,N}$, so using a different "distance measure" (i.e. only changing the first constraint in (9)) like $(\mathrm{tr}(\rho - \sigma))^2$ would not improve the analytic runtime (because the degree of the polynomial in the constraint is still 2), but may help in practice.

Another entanglement measure E that satisfies (11) is the *entanglement of formation* [39]

$$E_F(\rho) := \min_{\{p_i, |\psi_i\rangle\langle\psi_i|\}_i :\ \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|} \sum_i p_i S(\mathrm{tr}_{\mathrm{B}}(|\psi_i\rangle\langle\psi_i|)), \tag{12}$$

where $S(\rho) := -\mathrm{tr}(\rho \log(\rho))$ is the von Neumann entropy. This gives another strategy for a separability algorithm: search through all decompositions of the given ρ to find one that is separable. We can implement this strategy using the same relaxation technique of Eisert et al., but first we have to formulate the strategy as a polynomially-constrained optimization problem. The role of the function S is to measure the entanglement of $|\psi_i\rangle\langle\psi_i|$ by measuring the mixedness of the reduced state $\mathrm{tr}_{\mathrm{B}}(|\psi_i\rangle\langle\psi_i|)$. For our purposes, we can replace S with any other function T that measures mixedness such that, for all $\rho \in \mathcal{D}_{M,N}$, $T(\rho) \geq 0$ and $T(\rho) = 0$ if and only if ρ is pure. Recalling that, for any $\rho \in \mathcal{D}_{M,N}$, $\mathrm{tr}(\rho^2) \leq 1$ with equality if and only if ρ is pure, the function $T(\rho) := 1 - \mathrm{tr}(\rho^2)$ suffices; this function T may be written as a (finite-degree) polynomial in the real variables of ρ, whereas S could not. Defining

$$E'_F(\rho) := \min_{\{p_i, |\psi_i\rangle\langle\psi_i|\}_i :\ \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|} \sum_i p_i T(\mathrm{tr}_{\mathrm{B}}(|\psi_i\rangle\langle\psi_i|)), \tag{13}$$

we have that E'_F satisfies (11). Using an argument similar to the proof of Lemma 1 in [40], we can show that the minimum in (13) is attained by a *finite* decomposition of ρ into $M^2N^2 + 1$ pure states. Thus, the following polynomially-constrained optimization problem can be approximated by semidefinite relaxations:

$$\begin{array}{lrcl}
\text{minimize} & \multicolumn{3}{l}{\sum_{i=1}^{M^2N^2+1} \mathrm{tr}(X_i) T(\mathrm{tr}_{\mathrm{B}}(X_i))} \\
\text{subject to:} & \mathrm{tr}(\sum_{i=1}^{M^2N^2+1} X_i - [\rho])^2 & = & 0 \\
 & \mathrm{tr}(\sum_{i=1}^{M^2N^2+1} X_i) & = & 1 \\
 & \mathrm{tr}(X_i^2) & = & (\mathrm{tr}(X_i))^2, \\
 & & & \text{for } i = 1, 2, \ldots, M^2N^2 + 1 \\
 & \mathrm{tr}(X_i^3) & = & (\mathrm{tr}(X_i))^3, \\
 & & & \text{for } i = 1, 2, \ldots, M^2N^2 + 1.
\end{array} \tag{14}$$

The above has about half as many constraints as (9), so it would be interesting to compare the performance of the two approaches.

1.2.4 Other tests

There are several one-sided tests which do not lead to full algorithms for the quantum separability problem for $\mathcal{S}_{M,N}$.

Definition 3 (Robust semidefinite program) *Given the vector $c \in \mathbf{R}^m$, Hermitian matrices $F_i \in \mathbf{C}^{n\times n}$, $i = 0, 1, \ldots, m$, and vector space $\mathcal{D}$,*

$$\begin{aligned} &\textit{minimize} && c^T x && (15)\\ &\textit{subject to:} && F(x,\Delta) \geq 0, \textit{ for all } \Delta \in \mathcal{D}, && (16) \end{aligned}$$

where $F(x,\Delta) := F_0(\Delta) + \sum_{i=1}^{m} x_i F_i(\Delta)$.

Brandão and Vianna [41] have a set of one-sided necessary tests based on deterministic relaxations of a robust semidefinite program, but this set is not an asymptotically complete hierarchy. The same authors also have a related *randomized* quantum separability algorithm which uses probabilistic relaxations of the same robust semidefinite program [42] (but randomized algorithms are outside of our scope). I give their robust semidefinite program at the end of Section 3.3.1, where we will see a similar (nonrobust) SDP – essentially, a discretization of the robust semidefinite program – that solves the (approximate) quantum separability problem.

Woerdeman [43] has a set of one-sided tests for the case where $M = 2$. His approach might be described as the mirror-image of Doherty et al.'s: Instead of using an infinite hierarchy of necessary criteria for separability, he uses an infinite hierarchy of sufficient criteria. Each criterion in the hierarchy can be checked with a SDP.

2 Separability as a Computable Decision Problem

Definition 1 gave us a concrete definition of the quantum separability problem that we could use to explore some important results. Now we step back from that definition and, in Section 2.1, consider more carefully how we might formulate the quantum separability problem for the purposes of computing it. After considering exact formulations in Section 2.1.1, we settle on approximate formulations of the problem in Section 2.1.2, and give a few examples that are, in a sense, equivalent.

In Section 2.2, I discuss various aspects of the computational complexity of the quantum separability problem. Section 2.2.1 contains a review of NP-completeness theory. In Sections 2.2.2 and 2.2.3, I give a formulation of the quantum separability problem that is NP-complete with respect to Turing reductions. In Section 2.2.4, I consider the quantum separability problem's membership in co-NP. In Section 2.2.5, I explore the problem of strong NP-hardness of the (approximate) quantum separability problem. Finally, in Section 2.2.6, I discuss the open problem of whether the quantum separability problem is NP-complete with respect to Karp reductions.

2.1 Formulating the quantum separability problem

The nature of the quantum separability problem and the possibility for quantum computers allows a number of approaches, depending on whether the input to the problem is classical (a matrix representing ρ) or quantum (T copies of a physical system prepared in state ρ) and whether the processing of the input will be done on a classical computer or on a quantum computer. The use of entanglement witnesses[e] in the laboratory is a case of a quantum input and very limited quantum processing in the form of measurement of each copy of ρ. The case of more-sophisticated quantum processing on either a quantum or classical input is not well studied (see [44] for an instance of more-sophisticated quantum processing on a quantum input). For the remainder of the paper, I focus on the case where input and processing are classical (though the algorithm in Section 3.3 can be applied in an experimental setting [4, 5]).

2.1.1 Exact formulations

Let us examine Definition 1 from a computational viewpoint. The matrix $[\rho]$ is allowed to have real entries. Certainly there are real numbers that are uncomputable (e.g. a number whose nth binary digit is 1 if and only if the nth Turing machine halts on input n); we disallow such inputs. However, the real numbers e, π, and $\sqrt{2}$ are computable to any degree of approximation, so in principle they should be allowed to appear in $[\rho]$. In general, we should allow any real number that can be approximated arbitrarily well by a computer subroutine. If $[\rho]$ consists of such real numbers (subroutines), say that "ρ is given as an approximation algorithm for $[\rho]$." In this case, we have a procedure to which we can give an accuracy parameter $\delta > 0$ and out of which will be returned a matrix $[\rho]_\delta$ that is (in some norm) at most δ away from $[\rho]$. Because $\mathcal{S}_{M,N}$ is closed, the sequence $([\rho]_{1/n})_{n=1,2,...}$ may converge to a point on the boundary of $\mathcal{S}_{M,N}$ (when ρ is on the boundary of $\mathcal{S}_{M,N}$). For such ρ, the formal quantum separability problem may be "undecidable" because the δ-radius ball centred at $[\rho]_\delta$ may contain both separable and entangled states for all $\delta > 0$ [45] (more generally, see "Type II computability" in [46]).

If we really want to determine the complexity of deciding membership in $\mathcal{S}_{M,N}$, it makes sense not to confuse this with the complexity of specifying the input. To give the computer a fighting chance, it makes more sense to restrict to inputs that have finite exact representations that can be readily subjected to elementary arithmetic operations begetting exact answers. For this reason, we might restrict the formal quantum separability problem to instances where $[\rho]$ consists of rational entries:

Definition 4 (Rational quantum separability problem (EXACT QSEP)) *Let $\rho \in \mathcal{D}_{M,N}$ be a mixed state such that the matrix $[\rho]$ (with respect to the standard basis of $\mathbf{C}^M \otimes \mathbf{C}^N$) representing ρ consists of rational entries. Given $[\rho]$, is ρ separable?*

As pointed out in [2], Tarski's algorithm[f] [48] can be used to solve EXACT QSEP. The Tarski-approach is as follows. Note that the following first-order logical formula[g] is true if

[e] An *entanglement witness (for ρ)* is defined to be any operator $A \in \mathbf{H}_{M,N}$ such that $\mathrm{tr}(A\sigma) < \mathrm{tr}(A\rho)$ for all $\sigma \in \mathcal{S}_{M,N}$ and some $\rho \in \mathcal{E}_{M,N}$; we say that "$A$ detects ρ". Every $\rho \in \mathcal{E}_{M,N}$ has an entanglement witness that detects it [22].

[f] Tarski's result is often called the "Tarski-Seidenberg" theorem, after Seidenberg, who found a slightly better algorithm [47] (and elaborated on its generality) in 1954, shortly after Tarski managed to publish his; but Tarski discovered his own result in 1930 (the war prevented him from publishing before 1948).

[g] Recall the logical connectives: $\vee$ ("OR"), $\wedge$ ("AND"), $\neg$ ("NOT"); the symbol $\rightarrow$ ("IMPLIES"), in "$x \rightarrow y$", is a shorthand, as "$x \rightarrow y$" is equivalent to "$(\neg x) \vee y$"; as well, we can consider "$x \vee y$" shorthand for "$\neg((\neg x) \wedge (\neg y))$". Also recall the existential and universal quantifiers $\exists$ ("THERE EXISTS") and $\forall$ ("FOR ALL"); note that the universal quantifier $\forall$ is redundant as "$\forall x \phi(x)$" is equivalent to "$\neg \exists x \neg \phi(x)$".

and only if ρ is separable:

$$\forall A[(\forall \Psi(\mathrm{tr}(A\Psi) \geq 0)) \rightarrow (\mathrm{tr}A\rho \geq 0)], \tag{17}$$

where $A \in \mathbf{H}_{M,N}$ and Ψ is a pure product state. To see this, note that the subformula enclosed in square brackets means "$-A$ is not an entanglement witness for ρ", so that if this statement is true for all A then there exists no entanglement witness detecting ρ. When $[\rho]$ is rational, our experience in Section 1.2.2 with polynomial constraints tells us that the formula in (17) can be written in terms of "quantified polynomial inequalities" with rational coefficients:

$$\forall X\{(\forall Y\, [Q(Y) \rightarrow (r(X,Y) \geq 0)]) \rightarrow (s(X) \geq 0)\}, \tag{18}$$

where

- X is a block of real variables parametrizing the matrix $A \in \mathbf{H}_{M,N}$ (with respect to an orthogonal rational Hermitian basis of $\mathbf{H}_{M,N}$); the "Hermiticity" of X is hard-wired by the parametrization;
- Y is a block of real variables parametrizing the matrix Ψ;
- $Q(Y)$ is a conjunction of four polynomial equations that are equivalent to the four constraints $\mathrm{tr}((\mathrm{tr}_j(\Psi))^2) = 1$ and $\mathrm{tr}((\mathrm{tr}_j(\Psi))^3) = 1$ for $j \in \{\mathrm{A}, \mathrm{B}\}$;
- $r(X,Y)$ is a polynomial representing the expression $\mathrm{tr}(A\Psi)$;[h]
- $s(X)$ is a polynomial representing the expression $\mathrm{tr}(A[\rho])$.

The main point of Tarski's result is that the quantifiers (and variables) in the above sentence can be eliminated so that what is left is just a formula of elementary algebra involving Boolean connections of atomic formula of the form $(\alpha \diamond 0)$ involving terms α consisting of rational numbers, where $\diamond$ stands for any of $<, >, =, \neq$; the truth of the remaining (very long) formula can be computed in a straightforward manner. The best algorithms for deciding (18) require a number of arithmetic operations roughly equal to $(PD)^{O(|X|)\times O(|Y|)}$, where P is the number of polynomials in the input, D is the maximum degree of the polynomials, and $|X|$ ($|Y|$) denotes the number of variables in block X (Y) [49]. Since $P = 6$ and $D = 3$, the running time is roughly $2^{O(M^4N^4)}$.

2.1.2 Approximate formulations

The benefit of EXACT QSEP is that, compared to Definition 1, it eliminated any uncertainty in the input by disallowing irrational matrix entries. Consider the following motivation for an alternative to EXACT QSEP, where, roughly, we only ask whether the input $[\rho]$ corresponds to something *close to* separable:

[h] To ensure the Hermitian basis is rational, we do not insist that each of its elements has unit Euclidean norm. If the basis is $\{X_i\}_{i=0,1,\ldots,M^2N^2}$, where X_0 is proportional to the identity operator, then we can ignore the X_0 components write $A = \sum_{i=1}^{M^2N^2} A_i X_i$ and $\Psi = \sum_{i=1}^{M^2N^2} \Psi_i X_i$. An expression for $\mathrm{tr}(A\Psi)$ in terms of the real variables A_i and Ψ_i may then look like $\sum_{i=1}^{M^2N^2} A_i \Psi_i \mathrm{tr}(X_i^2)$.

- Suppose we really want to determine the separability of a density operator ρ such that $[\rho]$ has irrational entries. If we use the EXACT QSEP formulation (so far, we have no decidable alternative), we must first find a rational approximation to $[\rho]$. Suppose the (Euclidean) distance from $[\rho]$ to the approximation is δ. The answer that the Tarski-style algorithm gives us might be wrong, if ρ is not more than δ away from the boundary of $\mathcal{S}_{M,N}$.

- Suppose the input matrix came from measurements of many copies of a physical state ρ. Then we only know $[\rho]$ to some degree of approximation.

- The best known Tarski-style algorithms for EXACT QSEP have gigantic running times. Surely, we can achieve better asymptotic running times if we use an approximate formulation.

Thus, in many cases of interest, insisting that an algorithm says exactly whether the input matrix corresponds to a separable state is a waste of time. In Section 2.2.2, we will see that there is another reason to use an approximate formulation, if we would like the problem to fit nicely in the theory of NP-completeness.

Gurvits was the first to use the weak membership formulation of the quantum separability problem [50, 51]. For $x \in \mathbf{R}^n$ and $\delta > 0$, let $B(x,\delta) := \{y \in \mathbf{R}^n : ||x-y|| \leq \delta\}$. For a convex subset $K \subset \mathbf{R}^n$, let $S(K,\delta) := \cup_{x\in K} B(x,\delta)$ and $S(K,-\delta) := \{x : B(x,\delta) \subseteq K\}$.

Definition 5 (Weak membership problem for K (WMEM(K))) *Given a rational vector $p \in \mathbf{R}^n$ and rational $\delta > 0$, assert either that*

$$\begin{aligned} p &\in S(K,\delta), \quad \textit{or} && (19)\\ p &\notin S(K,-\delta). && (20) \end{aligned}$$

Denote by WMEM($\mathcal{S}_{M,N}$) the quantum separability problem formulated as the weak membership problem. An algorithm solving WMEM($\mathcal{S}_{M,N}$) is a separability test with two-sided "error" in the sense that it may assert (19) when p represents an entangled state and may assert (20) when p represents a separable state. Any formulation of the quantum separability problem will have (at least) two possible answers – one corresponding to "p approximately represents a separable state" and the other corresponding to "p approximately represents an entangled state". Like in WMEM($\mathcal{S}_{M,N}$), there may be a region of p where both answers are valid. We can use a different formulation where this region is shifted to be either completely outside $\mathcal{S}_{M,N}$ or completely inside $\mathcal{S}_{M,N}$:

Definition 6 (In-biased weak membership problem for K (WMEM$_{\mathbf{In}}$(K))) *Given a rational vector $p \in \mathbf{R}^n$ and rational $\delta > 0$, assert either that*

$$\begin{aligned} p &\in S(K,\delta), \quad \textit{or} && (21)\\ p &\notin K. && (22) \end{aligned}$$

Definition 7 (Out-biased weak membership problem for K ($\mathbf{WMEM_{Out}}(K)$)) *Given a rational vector $p \in \mathbf{R}^n$ and rational $\delta > 0$, assert either that*

$$\begin{aligned} p &\in K, \quad \textit{or} \qquad (23)\\ p &\notin S(K,-\delta). \qquad (24) \end{aligned}$$

We can also formulate a "zero-error" version such that when p is in such a region, then any algorithm for the problem has the option of saying so, but otherwise must answer exactly:

Definition 8 (Zero-error weak membership problem for K ($\mathbf{WMEM}^0(K)$)) *Given a rational vector $p \in \mathbf{R}^n$ and rational $\delta > 0$, assert either that*

$$\begin{aligned} p &\in K, \quad \textit{or} \qquad (25)\\ p &\notin K, \quad \textit{or} \qquad (26)\\ p &\in S(K,\delta) \setminus S(K,-\delta) \qquad (27) \end{aligned}$$

All the above formulations of the quantum separability problem are based on the Euclidean norm and use the isomorphism between $\mathbf{H}_{M,N}$ and $\mathbf{R}^{M^2N^2}$. We could also make similar formulations based on other operator norms in $\mathbf{H}_{M,N}$. In the next section, we will see yet another formulation of an entirely different flavour. While each formulation is slightly different, they all have the property that in the limit as the error parameter approaches 0, the problem coincides with EXACT QSEP. Thus, despite the apparent inequivalence of these formulations, we recognize that they all basically do the same job. In fact, WMEM($\mathcal{S}_{M,N}$), WMEM$_{\text{In}}$($\mathcal{S}_{M,N}$), WMEM$_{\text{Out}}$($\mathcal{S}_{M,N}$), and WMEM$(\mathcal{S}_{M,N})^0$ are equivalent: given an algorithm for one of the problems, one can solve an instance (ρ,δ) of any of the other three problems by just calling the given algorithm at most twice (with various parameters).[i]

2.2 Computational complexity

This section addresses how the quantum separability problem fits into the framework of complexity theory. I assume the reader is familiar with concepts such as *problem*, *instance* (of a problem), *(reasonable, binary) encodings*, *polynomially relatedness*, *size* (of an instance), *(deterministic and nondeterministic) Turing machine*, and *polynomial-time algorithm*; all of which can be found in any of [53, 54, 55].

Generally, the weak membership problem is defined for a class $\mathcal{K}$ of convex sets. For example, in the case of WMEM($\mathcal{S}_{M,N}$), this class is $\{\mathcal{S}_{M,N}\}_{M,N}$ for all integers M and N

[i] To show this equivalence, it suffices to show that given an algorithm for WMEM($\mathcal{S}_{M,N}$), one can solve WMEM$_{\text{Out}}$($\mathcal{S}_{M,N}$) with one call to the given algorithm (the converse is trivial); a similar proof shows that one can solve WMEM$_{\text{In}}$($\mathcal{S}_{M,N}$) with one call to the algorithm for WMEM($\mathcal{S}_{M,N}$). The other relationships follow immediately. Let (ρ,δ) be the given instance of WMEM$_{\text{Out}}$($\mathcal{S}_{M,N}$). Define $\rho_0 := \rho + \delta(\rho - I_{M,N})/2$ and $\delta_0 := \delta/(2\sqrt{MN(MN-1)})$. Call the algorithm for WMEM($\mathcal{S}_{M,N}$) with input (ρ_0,δ_0). Suppose the algorithm asserts $\rho_0 \notin S(\mathcal{S}_{M,N},-\delta_0)$. Then, because $||\rho-\rho_0|| = \frac{\delta}{2}||\rho - I_{M,N}||$ and $||\rho - I_{M,N}|| \leq 1$, we have $\rho \notin S(\mathcal{S}_{M,N}, -(\delta_0 + \delta/2))$ hence $\rho \notin S(\mathcal{S}_{M,N},-\delta)$. Otherwise, suppose the algorithm asserts $\rho_0 \in S(\mathcal{S}_{M,N},\delta_0)$. By way of contradiction, assume that ρ is entangled. But then, by convexity of $\mathcal{S}_{M,N}$ and the fact that $\mathcal{S}_{M,N}$ contains the ball $B(I_{M,N}, 1/\sqrt{MN(MN-1)})$, we can derive that the ball $B(\rho_0,\delta_0)$ does not intersect $\mathcal{S}_{M,N}$. But this implies $\rho_0 \notin S(\mathcal{S}_{M,N},\delta_0)$ – a contradiction. Thus, $\rho \in \mathcal{S}_{M,N}$. This proof is a slight modification of the argument given in [52]. See also Lemma 4.3.3 in [50].

such that $2 \leq M \leq N$. An instance of WMEM thus includes the specification of a member K of $\mathcal{K}$. The size of an instance must take into account the size $\langle K \rangle$ of the encoding of K. It is reasonable that $\langle K \rangle \geq n$ when $K \in \mathbf{R}^n$, because an algorithm for the problem should be able to work efficiently (in time that is upper-bounded by a polynomial in the size of an instance) with points in $\mathbf{R}^n$. But the complexity of K matters, too. For example, if K extends (doubly-exponentially) far from the origin (but contains the origin) then K may contain points that require large amounts of precision to represent; again, an algorithm for the problem should be able to work with such points efficiently (for example, it should be able to add such a point and a point close to the origin, and store the result efficiently). In the case of WMEM($\mathcal{S}_{M,N}$), the size of the encoding of $\mathcal{S}_{M,N}$ may be taken as N (assuming $M \leq N$), as $\mathcal{S}_{M,N}$ is not unreasonably long or unreasonably thin: it is contained in the unit sphere in $\mathbf{R}^{M^2N^2-1}$ and contains a ball of separable states of radius $\Omega(1/\text{poly}(N))$ (see Section 1.1).[j] Thus, the total size of an instance of WMEM($\mathcal{S}_{M,N}$), or any formulation of the quantum separability problem, may also be taken to be N plus the size of the encoding of (ρ, δ).

2.2.1 Review of NP-completeness

Complexity theory, and, particularly, the theory of NP-completeness, pertains to *decision problems* – problems that pose a yes/no question. Let Π be a decision problem. Denote by D_Π the set of instances of Π, and denote the yes-instances of Π by Y_Π. Recall that the complexity class P (respectively, NP) is the set of all problems the can be decided by a deterministic Turing machine (respectively, nondeterministic Turing machine) in polynomial time. The following equivalent definition of NP is perhaps more intuitive:

Definition 9 (NP) *A decision problem Π is in NP if there exists a deterministic Turing machine T_Π such that for every instance $I \in \mathrm{Y}_\Pi$ there exists a string C_I of length $|C_I| \in O(poly(|I|))$ such that T_Π, with inputs C_I and (an encoding of) I, can check that I is in Y_Π in time $O(poly(|I|))$.*

The string C_I is called a *(succinct) certificate.* Let Π^c be the complementary problem of Π, i.e. $\mathrm{D}_{\Pi^c} \equiv \mathrm{D}_\Pi$ and $\mathrm{Y}_{\Pi^c} := \mathrm{D}_\Pi \setminus \mathrm{Y}_\Pi$. The class co-NP is thus defined as $\{\Pi^c : \ \Pi \in \mathrm{NP}\}$.

Let us briefly review the different notions of "polynomial-time reduction" from one problem Π' to another Π. Let $\mathcal{O}_\Pi$ be an oracle, or black-boxed subroutine, for solving Π, to which we assign unit complexity cost. A *(polynomial-time) Turing reduction* from Π' to Π is any polynomial-time algorithm for Π' that makes calls to $\mathcal{O}_\Pi$. Write $\Pi' \leq_\mathrm{T} \Pi$ if Π' is Turing-reducible to Π. A *polynomial-time transformation*, or *Karp reduction*, from Π' to Π is a Turing reduction from Π' to Π in which $\mathcal{O}_\Pi$ is called at most once and at the end of the reduction algorithm, so that the answer given by $\mathcal{O}_\Pi$ is the answer to the given instance of Π'. In other words, a Karp reduction from Π' to Π is a polynomial-time algorithm that (under a reasonable encoding) takes as input an (encoding of an) instance I' of Π' and outputs an (encoding of an) instance I of Π such that $I' \in \mathrm{Y}_{\Pi'} \Leftrightarrow I \in \mathrm{Y}_\Pi$. Write $\Pi' \leq_\mathrm{K} \Pi$ if Π' is Karp-reducible to Π. Karp and Turing reductions are on the extreme ends of a spectrum of polynomial-time reductions; see [56] for a comparison of several of them.

[j] Recall that a function $f(n)$ is in $\Omega(g(n))$ when there exist constants c and n_0 such that $cg(n) \leq f(n)$ for all $n > n_0$.

Reductions between problems are a way of determining how hard one problem is relative to another. The notion of NP-completeness is meant to define the hardest problems in NP. We can define NP-completeness with respect to any polynomial-time reduction; we define *Karp-NP-completeness* and *Turing-NP-completeness*:

$$\mathrm{NPC}_{\mathrm{K}} := \{\Pi \in \mathrm{NP} : \ \Pi' \leq_{\mathrm{K}} \Pi \text{ for all } \Pi' \in \mathrm{NP}\ \} \tag{28}$$

$$\mathrm{NPC}_{\mathrm{T}} := \{\Pi \in \mathrm{NP} : \ \Pi' \leq_{\mathrm{T}} \Pi \text{ for all } \Pi' \in \mathrm{NP}\ \}. \tag{29}$$

We have $\mathrm{NPC}_{\mathrm{K}} \subseteq \mathrm{NPC}_{\mathrm{T}}$. Let Π, Π', and Π'' be problems in NP, and, furthermore, suppose Π' is in $\mathrm{NPC}_{\mathrm{K}}$. If $\Pi' \leq_{\mathrm{T}} \Pi$, then, in a sense, Π is at least as hard as Π' (which gives an interpretation of the symbol "$\leq_{\mathrm{T}}$"). Suppose $\Pi' \leq_{\mathrm{T}} \Pi$ but suppose also that Π' is not Karp-reducible to Π. If $\Pi' \leq_{\mathrm{K}} \Pi''$, then we can say that "$\Pi''$ is at least as hard as Π", because, to solve Π' (and thus any other problem in NP), $\mathcal{O}_{\Pi}$ has to be used at least as many times as $\mathcal{O}_{\Pi''}$; if any Turing reduction proving $\Pi' \leq_{\mathrm{T}} \Pi$ requires more than one call to $\mathcal{O}_{\Pi}$, then we can say "Π'' is harder than Π". Therefore, if $\mathrm{NPC}_{\mathrm{K}} \neq \mathrm{NPC}_{\mathrm{T}}$, then the problems in $\mathrm{NPC}_{\mathrm{K}}$ are harder than the problems in $\mathrm{NPC}_{\mathrm{T}} \setminus \mathrm{NPC}_{\mathrm{K}}$; thus $\mathrm{NPC}_{\mathrm{K}}$ are the hardest problems in NP (with respect to polynomial-time reductions).

A problem Π is *NP-hard* when $\Pi' \leq_{T} \Pi$ for some Karp-NP-complete problem $\Pi' \in \mathrm{NPC}_{\mathrm{K}}$. The term "NP-hard" is also used for problems other than decision problems. For example, let $\Pi' \in \mathrm{NPC}_{\mathrm{K}}$; then $\mathrm{WMEM}(\mathcal{S}_{M,N})$ is NP-hard if there exists a polynomial-time algorithm for Π' that calls $\mathcal{O}_{\mathrm{WMEM}(\mathcal{S}_{M,N})}$.

2.2.2 Quantum separability problem in NP

Fact 1 suggests that the quantum separability problem is in NP: a nondeterministic Turing machine guesses $\{(p_i, [|\psi_i^{\mathrm{A}}\rangle], [|\psi_i^{\mathrm{B}}\rangle])\}_{i=1}^{M^2N^2}$,[k] and then easily checks that

$$[\rho] = \sum_{i=1}^{M^2N^2} p_i [|\psi_i^{\mathrm{A}}\rangle][\langle\psi_i^{\mathrm{A}}|] \otimes [|\psi_i^{\mathrm{B}}\rangle][\langle\psi_i^{\mathrm{B}}|]. \tag{30}$$

Technically, membership in NP is only defined for decision problems. Since none of the weak membership formulations of the quantum separability problem can be rephrased as decision problems (because problem instances corresponding to states near the boundary of $\mathcal{S}_{M,N}$ can satisfy both possible answers), we cannot consider their membership in NP (but see Section 2.2.4, where we define NP for promise problems). However, EXACT QSEP *is* a decision problem.

Problem 1 *Is* EXACT QSEP *in* NP*?*

Hulpke and Bruß [57] have formalized some important notions related to this problem. They show that if $\rho \in S(\mathcal{S}_{M,N}, -\delta)$, for some $\delta > 0$, then each of the extreme points $x_i \in \mathcal{S}_{M,N}$ in the expression $\rho = \sum_{i=1}^{M^2N^2} p_i x_i$ can be replaced by $\tilde{x}_i$, where $[\tilde{x}_i]$ has rational entries. This is possible because the extreme points (pure product states) of $\mathcal{S}_{M,N}$ with rational entries are dense in the set of all extreme points of $\mathcal{S}_{M,N}$. However, when $\rho \notin S(\mathcal{S}_{M,N}, -\delta)$, then this argument breaks down. For example, when ρ has full rank and is on the boundary of

[k] I use square brackets to denote a matrix with respect to the standard basis.

$\mathcal{S}_{M,N}$, then "sliding" x_i to a rational position $\tilde{x}_i$ might cause $\tilde{x}_i$ to be outside of the affine space generated by $\{x_i\}_{i=1,\ldots,k}$. Figure 1 illustrates this in $\mathbf{R}^3$. Furthermore, even if x_i can be nudged comfortably to a rational $\tilde{x}_i$, one would have to prove that $\langle \tilde{x}_i \rangle \in O(\text{poly}(\langle [\rho] \rangle))$, where $\langle X \rangle$ is the size of the encoding of X.

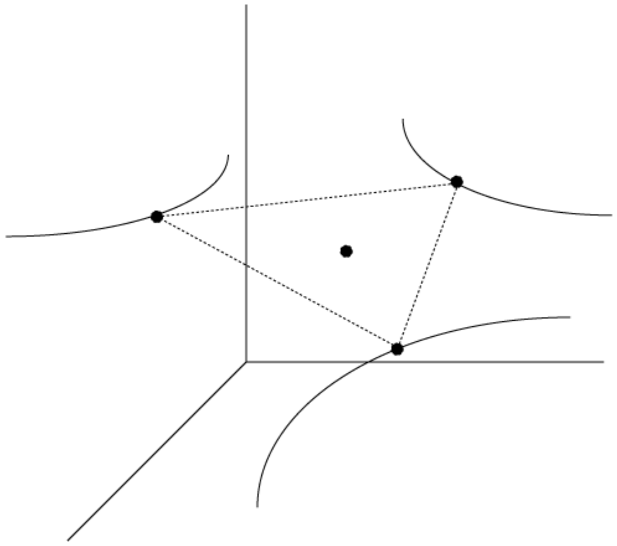

Fig. 1. The dashed triangle outlines the convex hull of x_1, x_2, and x_3, shown as dots at the triangle's vertices. This convex hull contains ρ, shown as a dot inside the triangle, and forms a (schematic) face of $\mathcal{S}_{M,N}$. The curves represent the allowable choices for the $\tilde{x}_i$. Sliding any of the x_i takes $\text{conv}\{x_1, x_2, x_3\}$ outside of the face. Incidentally, $\mathcal{S}_{M,N}$ has no maximum-dimensional faces (facets); this follows from results in [58].

So, either the definition of NP does not apply (for weak membership formulations), or we possibly run into problems near the boundary of $\mathcal{S}_{M,N}$ (for exact formulations). Below we give an alternative formulation that is in NP; we will refer to this problem as QSEP. The definition of QSEP is just a precise formulation of the question "Given a density operator ρ, does there exist a separable density operator $\hat{\sigma}$ that is close to ρ?"

Definition 10 (QSEP) *Given a rational density matrix $[\rho]$ of dimension MN-by-MN, and positive rational numbers δ_p, ϵ' and δ'; does there exist a distribution $\{(\tilde{p}_i; \tilde{\alpha}_i, \tilde{\beta}_i)\}_{i=1,2,\ldots,M^2N^2}$ of unnormalized pure states $\tilde{\alpha}_i \in \mathbf{C}^M$, $\tilde{\beta}_i \in \mathbf{C}^N$ where $\tilde{p}_i \geq 0$, and $\tilde{p}_i$ and all elements of $\tilde{\alpha}_i$ and $\tilde{\beta}_i$ are $\lceil \log_2(1/\delta_p) \rceil$-bit numbers (complex elements are $x + iy$, $x, y \in \mathbf{R}$; where x and y are $\lceil \log_2(1/\delta_p) \rceil$-bit numbers) such that*

$$\left| 1 - ||\tilde{\alpha}_i||^2 ||\tilde{\beta}_i||^2 \sum_{j=1}^{M^2N^2} \tilde{p}_j \right| < \epsilon' \quad \textit{for all } i \tag{31}$$

and

$$||[\rho] - \tilde{\sigma}||_2^2 := tr(([\rho] - \tilde{\sigma})^2) < \delta'^2, \tag{32}$$

where $\tilde{\sigma} := \sum_{i=1}^{M^2N^2} \tilde{p}_i \tilde{\alpha}_i \tilde{\alpha}_i^\dagger \otimes \tilde{\beta}_i \tilde{\beta}_i^\dagger$*?*

Note that these checks can be done exactly in polynomial-time, as they only involve elementary arithmetic operations on rational numbers. To reconcile this definition with the above question, we define $\hat{\sigma}$ as the separable density matrix that is the "normalized version" of $\tilde{\sigma}$:

$$\hat{\sigma} := \sum_{i=1}^{M^2N^2} \hat{p}_i \hat{\alpha}_i \hat{\alpha}_i^\dagger \otimes \hat{\beta}_i \hat{\beta}_i^\dagger, \tag{33}$$

where $\hat{p}_i := \tilde{p}_i / \sum_i \tilde{p}_i$, $\hat{\alpha}_i := \tilde{\alpha}_i / ||\tilde{\alpha}_i||$, and $\hat{\beta}_i := \tilde{\beta}_i / ||\tilde{\beta}_i||$. Using the triangle inequality, we can derive that

$$||\hat{\sigma} - \tilde{\sigma}||_2 \leq \sum_i \hat{p}_i \left| 1 - ||\tilde{\alpha}_i||^2 ||\tilde{\beta}_i||^2 \sum_j \tilde{p}_j \right|, \tag{34}$$

where the righthand side is less than ϵ' when (31) is satisfied. If (32) is also satisfied, then we have

$$||[\rho] - \hat{\sigma}||_2 \leq ||[\rho] - \tilde{\sigma}||_2 + ||\hat{\sigma} - \tilde{\sigma}||_2 \leq \delta' + \epsilon', \tag{35}$$

which says that the given $[\rho]$ is no further than $\delta' + \epsilon'$ away from a separable density matrix (in Euclidean norm).[l]

The decision problem QSEP is trivially in NP, as a nondeterministic Turing machine need only guess the $\lceil \log_2(1/\delta_p) \rceil$-bit distribution $\{(\tilde{p}_i; \tilde{\alpha}_i, \tilde{\beta}_i)\}_{i=1,2,\ldots,M^2N^2}$ and verify (in polytime) that (31) and (32) are satisfied.

2.2.3 NP-Hardness

Gurvits has shown WMEM($\mathcal{S}_{M,N}$) to be NP-hard (with respect to the complexity-measures M and $\langle \delta \rangle$, i.e. $\min\{M, N\}$ and $1/\delta$ must be allowed to increase) [51]. More details about this result appear in Section 2.2.5.

We check now that QSEP is NP-hard, by way of a Karp-reduction from WMEM($\mathcal{S}_{M,N}$). We assume we are given an instance $I := ([\rho], \delta)$ of WMEM($\mathcal{S}_{M,N}$) and we seek an instance $I' := ([\rho'], \delta_p, \epsilon', \delta')$ of QSEP such that if I' is a "yes"-instance of QSEP, then I satisfies (19); otherwise I satisfies (20). It suffices to use $[\rho'] = [\rho]$. It is clear that if δ' and ϵ' are chosen such that $\delta \geq \delta' + \epsilon'$, then I' is a "yes"-instance only if I satisfies (19). For the other implication, we need to bound the propagation of some truncation-errors. Let $p := \lceil \log_2(1/\delta_p) \rceil$.

Recall how absolute errors accumulate when multiplying and adding numbers. Let $x = \tilde{x} + \Delta_x$ and $y = \tilde{y} + \Delta_y$ where x, y, $\tilde{x}$, $\tilde{y}$, Δ_x, and Δ_y are all real numbers. Then we have

$$\begin{aligned} xy &= \tilde{x}\tilde{y} + \tilde{x}\Delta_y + \tilde{y}\Delta_x + \Delta_x\Delta_y && (36) \\ x + y &= \tilde{x} + \tilde{y} + \Delta_x + \Delta_y. && (37) \end{aligned}$$

For $|\tilde{x}|, |\tilde{y}| < 1$, because we will be dealing with summations of products with errors, it is sometimes convenient just to use

$$|xy - \tilde{x}\tilde{y}| \leq |\Delta_y| + |\Delta_x| + \max\{|\Delta_x|, |\Delta_y|\} \tag{38}$$

[l] I have formulated these checks to avoid division; this makes the error analysis of the next section simpler.

to obtain our cumulative errors (which do not need to be tight to show NP-hardness). For example, if $\tilde{x}$ and $\tilde{y}$ are the p-bit truncations of x and y, where $|x|, |y| < 1$, then $|\Delta_x|, |\Delta_y| < 2^{-p}$; thus a conservative bound on the error of $\tilde{x}\tilde{y}$ is

$$|xy - \tilde{x}\tilde{y}| < |\Delta_y| + |\Delta_x| + |\Delta_x| = 3|\Delta_x| < 2^2|\Delta_x| = 2^{-(p-2)}. \tag{39}$$

Proposition 1 *Let $\sigma \in \mathcal{S}_{M,N}$ be such that $\sigma = \sum_{i=1}^{M^2N^2} p_i\alpha_i\alpha_i^\dagger \otimes \beta_i\beta_i^\dagger$, and let $\{(\tilde{p}_i; \tilde{\alpha}_i, \tilde{\beta}_i)\}_{i=1,2,\ldots,M^2N^2}$ be the p-bit truncation of $\{(p_i; \alpha_i, \beta_i)\}_{i=1,2,\ldots,M^2N^2}$. Then $||\sigma - \tilde{\sigma}||_2 < M^3N^32^{-(p-7.5)}$, where*

$$\tilde{\sigma} := \sum_{i=1}^{M^2N^2} \tilde{p}_i\tilde{\alpha}_i\tilde{\alpha}_i^\dagger \otimes \tilde{\beta}_i\tilde{\beta}_i^\dagger. \tag{40}$$

Proof Letting $\gamma_i := p_i\alpha_i\alpha_i^\dagger \otimes \beta_i\beta_i^\dagger - \tilde{p}_i\tilde{\alpha}_i\tilde{\alpha}_i^\dagger \otimes \tilde{\beta}_i\tilde{\beta}_i^\dagger$, we use the triangle inequality to get

$$||\sigma - \tilde{\sigma}||_2 \quad \leq \quad \sum_i ||\gamma_i||_2 = \sum_i \sqrt{\mathrm{tr}(\gamma_i^2)}. \tag{41}$$

It suffices to bound the absolute error on the elements of $[\tilde{p}_i\tilde{\alpha}_i\tilde{\alpha}_i^\dagger \otimes \tilde{\beta}_i\tilde{\beta}_i^\dagger]$; using our conservative rule (38), these elements have absolute error less than $2^{-(p-7)}$. Thus $[\gamma_i]$ is an MN-by-MN matrix with elements no larger than $2^{-(p-7)}$ in absolute value. It follows that $(\mathrm{tr}(\gamma_i^2))^{1/2}$ is no larger than $\sqrt{MN}2^{-(p-7.5)}$ in absolute value. Finally, we get

$$||\sigma - \tilde{\sigma}||_2 \leq \sum_i \sqrt{\mathrm{tr}(\gamma_i^2)} \leq M^3N^32^{-(p-7.5)}.\square \tag{42}$$

Proposition 2 *Let $\tilde{\sigma}$ be as in Proposition 1. Then for all $i = 1, 2, \ldots M^2N^2$*

$$\left| 1 - ||\tilde{\alpha}_i||^2||\tilde{\beta}_i||^2 \sum_{j=1}^{M^2N^2} \tilde{p}_j \right| < M^3N^32^{-(p-5)}. \tag{43}$$

Proof The absolute error on $\sum_j \tilde{p}_j$ is $M^2N^22^{-p}$. The absolute error on $||\tilde{\alpha}_i||^2$ (resp. $||\tilde{\beta}_i||^2$) is no more than $M2^{-(p-3)}$ (resp. $N2^{-(p-3)}$). This gives total absolute error of

$$\left| 1 - ||\tilde{\alpha}_i||^2||\tilde{\beta}_i||^2 \sum_j \tilde{p}_j \right| < M^3N^32^{-(p-5)}.\square \tag{44}$$

Let $\delta' := M^3N^32^{-(p-8)}$ and $\epsilon' := M^3N^32^{-(p-5)}$ and set p such that $\epsilon' + \delta' \leq \delta$. Suppose there exists a separable density matrix σ such that $||[\rho] - \sigma||_2 = 0$. Then Propositions 1 and 2 say that there exists a certificate $\tilde{\sigma}$ such that (31) and (32) are satisfied. Therefore, if I' is a "no"-instance, then for all separable density matrices σ, $||[\rho] - \sigma||_2 > 0$; which implies that I satisfies (20). This concludes a polytime Karp-reduction from WMEM($\mathcal{S}_{M,N}$) to QSEP (actually, from WMEM$_{\mathrm{In}}$($\mathcal{S}_{M,N}$) to QSEP):

Fact 3 QSEP *is in* NPC$_{\mathrm{T}}$.

2.2.4 Nonmembership in co-NP

Technically, WMEM($\mathcal{S}_{M,N}$) is not in NP because it is not a decision problem; but it is a promise problem. Recall that a *promise problem* Π may be defined as a generalization of a decision problem, where, instead of just yes-instances Y_Π and no-instances N_Π, we allow a third set of maybe-instances (the "promise" is that the given instance is in $\mathrm{Y}_\Pi \cup \mathrm{N}_\Pi$). For $\Pi = \mathrm{WMEM}(\mathcal{S}_{M,N})$, we have $\mathrm{Y}_\Pi = \{(x,\delta) : x \in S(\mathcal{S}_{M,N}, -\delta), \delta > 0\}$ and $\mathrm{N}_\Pi = \{(x,\delta) : x \in \mathcal{D}_{M,N} \setminus S(\mathcal{S}_{M,N}, \delta), \delta > 0\}$ (where we have implicitly restricted all states to being rational density matrices $[\rho]$). For our purposes, a promise problem Π is defined to be in *Promise-NP* if every yes-instance has a succinct certificate of being a yes-instance or a maybe-instance. Accordingly, WMEM($\mathcal{S}_{M,N}$) is clearly in Promise-NP.

Is either EXACT QSEP or QSEP in co-NP? To avoid possible technicalities, we might first consider the presumably easier question of whether WMEM($\mathcal{S}_{M,N}$) is in Promise-co-NP: Does every entangled state $\rho \notin S(\mathcal{S}_{M,N}, \delta)$ have a succinct certificate of not being in $S(\mathcal{S}_{M,N}, -\delta)$? It may or may not be the case that P equals NP∩co-NP, but a problem's membership in NP∩co-NP can be "regarded as suggesting" that the problem is in P [53]. Thus, we might believe that WMEM($\mathcal{S}_{M,N}$) is not in Promise-co-NP (since WMEM($\mathcal{S}_{M,N}$) is NP-hard).

Let us consider this with regard to entanglement witnesses, which are candidates for succinct certificates of entanglement. We know that every entangled state has an entanglement witness $A \in \mathbf{H}_{M,N}$ that detects it (see footnote on page 10). However, it follows from the NP-hardness of WMEM($\mathcal{S}_{M,N}$) and Theorem 4.4.4 in [50] that the weak validity problem for $K = \mathcal{S}_{M,N}$ (WVAL($\mathcal{S}_{M,N}$)) is NP-hard:[m]

Definition 11 (Weak validity problem for K (WVAL(K))) *Given a rational vector $c \in \mathbf{R}^n$, a rational number γ, and rational $\epsilon > 0$, assert either that*

$$c^T x \leq \gamma + \epsilon \textit{ for all } x \in K, \quad \textit{or} \tag{45}$$

$$c^T x \geq \gamma - \epsilon \textit{ for some } x \in K. \tag{46}$$

So there is no known way to check efficiently that a hyperplane $\pi_{A,b}$ separates ρ from $\mathcal{S}_{M,N}$ (given just the hyperplane); thus, an entanglement witness alone does not serve as a succinct certificate of a state's entanglement unless WVAL($\mathcal{S}_{M,N}$) is polytime solvable. However, one could imagine that there is a succinct certificate of the fact that a hyperplane $\pi_{A,b}$ separates ρ from $\mathcal{S}_{M,N}$. If such a certificate exists, then WVAL($\mathcal{S}_{M,N}$) is in Promise-NP (and thus WMEM($\mathcal{S}_{M,N}$) is in Promise-co-NP).[n]

With regard to QSEP, we have the following:

Fact 4 *QSEP is not in co-NP, unless NP equals co-NP.*

This follows from the fact that if any Turing-NP-complete problem is in co-NP, then NP equals co-NP [54]. It is strongly conjectured that NP and co-NP are different [54], thus we

[m] Theorem 4.4.4 in [50], applied to $\mathcal{S}_{M,N}$, states that there exists an oracle-polynomial-time algorithm that solves the WSEP($\mathcal{S}_{M,N}$) given an oracle for WVAL($\mathcal{S}_{M,N}$).

[n] WVAL(K) is in Promise-NP if, for any instance c, γ, ϵ satisfying $c^T x \leq \gamma - \epsilon$ for all $x \in K$, there exists a succinct certificate of the fact that $c^T x \leq \gamma + \epsilon$ for all $x \in K$.

might believe that QSEP is not in co-NP. We would like to be able to use Fact 4 to show that WVAL($\mathcal{S}_{M,N}$) is not in Promise-NP unless NP equals co-NP. However, for this, we would require that WVAL($\mathcal{S}_{M,N}$) is in Promise-NP implies QSEP is in co-NP; but this is not the case, because exhibiting a separating hyperplane for ρ (i.e. showing that ρ is entangled) does not make ρ a no-instance of QSEP.

2.2.5 Strong NP-hardness

The NP-complete problem known as PARTITION may be defined as follows: Given a nonnegative integral vector $a \in \mathbf{Z}^n$, does there exist a solution $z \in \{-1, 1\}^n$ to the equation $a^T z = 0$? It is well known that there exists a "dynamic programming" algorithm that solves PARTITION in time $O(\text{poly}(n||a||_1))$, where $||a||_1$ is the sum of the elements of a [53]. This is known as a *pseudopolynomial-time algorithm*, because *if* a is restricted such that $||a||_1 \in O(\text{poly}(n))$, *then* the algorithm runs in "polynomial time".

Aaronson [59] notes that Gurvits' original NP-hardness result (in [51]) more precisely shows that WMEM($\mathcal{S}_{M,N}$) is NP-hard provided that $1/\delta$ is exponentially large, as I briefly explain now. For this section only, we switch convention: $M \geq N$. The full reduction chain that Gurvits uses to prove NP-hardness is

$$\text{PARTITION} \leq_{\text{K}} \text{RSDF} \leq_{\text{K}} \text{WVAL}(\mathcal{S}_{M,N}) \leq_{\text{T}} \text{WMEM}(\mathcal{S}_{M,N}), \tag{47}$$

where the robust semidefinite feasibility (RSDF) problem is defined as follows:

Definition 12 (RSDF) *Given k $l \times l$, rational, symmetric matrices $B_1, \ldots, B_k$ and rational numbers ζ and η, assert either that*

$$F(B_1, \ldots, B_k) \leq \zeta + \eta, \quad or \tag{48}$$

$$F(B_1, \ldots, B_k) \geq \zeta - \eta, \tag{49}$$

where $F(B_1, \ldots, B_k) := \max_{x \in \mathbf{R}^l, ||x||_2 = 1} \sum_{i'=1}^{k} (x^T B_{i'} x)^2$.

Given a PARTITION instance $a \in \mathbf{Z}^l$, we want to solve it using an oracle for RSDF. The reduction (in [60]) from PARTITION to RSDF says that η needs to be on the order of $1/\text{poly}(l||a||_2)$. But this implies that, for a to be an NP-hard instance of PARTITION, $1/\eta$ needs to be exponentially large in l. In other words, WVAL($\mathcal{S}_{M,N}$) (and hence WMEM($\mathcal{S}_{M,N}$)) is only shown to be NP-hard when the accuracy parameter is very small. It is still conceivable, though, that WVAL($\mathcal{S}_{M,N}$) (resp. WMEM($\mathcal{S}_{M,N}$)) is tractable when $1/\epsilon$ (resp. $1/\delta$) is in $O(\text{poly}(M, N))$. Below, I show that a new reduction discovered by Gurvits [61] (inspired by the proof of Lemma 3 in [62]) removes the possibility for such a family of WVAL($\mathcal{S}_{M,N}$) instances in a certain regime of ϵ; moreover, I also remove this possibility for a problem slightly more difficult than the weak membership problem for $\mathcal{S}_{M,N}$.

The new reduction chain is

$$\text{CLIQUE} \leq_{\text{K}} \text{WMQS} \leq_{\text{K}} \text{RSDF} \leq_{\text{K}} \text{WVAL}(\mathcal{S}_{M,N}) \leq_{\text{T}} \text{WMEM}(\mathcal{S}_{M,N}), \tag{50}$$

where CLIQUE $\in$ NPC$_{\text{K}}$ (see [53]) is the problem of deciding whether the number of vertices in the largest complete subgraph (clique) of a given simple graph on n vertices is at least c

(given also integer $c \leq n$), and WMQS is the problem of weakly deciding a bound on the maximum of the quadratic form $y^T Ay$ over the simplex $\Delta_n := \{y \in \mathbf{R}^n : y_i \geq 0, ||y||_1 = 1\}$:

Definition 13 (WMQS) *Given rational, symmetric $A \in \mathbf{R}^{n \times n}$ with nonnegative entries A_{ij} and rational numbers ζ' and $\eta' > 0$, assert either that*

$$\begin{aligned} H(A) &\leq \zeta' + \eta', \quad \text{or} & (51)\\ H(A) &\geq \zeta' - \eta', & (52)\end{aligned}$$

where $H(A) := \max_{y \in \Delta_n} y^T Ay$.

The first link in this chain is well known via the following theorem:[o]

Theorem 1 ([63]) *Let G be a simple graph on n vertices, and let A_G be the adjacency matrix for G.*[p] *Let κ be the size of the maximum complete subgraph of G. Then*

$$\max_{y \in \Delta_n} y^T A_G y = 1 - 1/\kappa. \tag{53}$$

Suppose (G, c) is a given CLIQUE instance, where G has n vertices. To transform (G, c) into a WMQS-instance, just set ζ' to be the midpoint of interval $I_c = [1 - 1/(c-1), 1 - 1/c]$ and set η' so that the interval $[\zeta' - \eta', \zeta' + \eta']$ is strictly contained in I_c (and set $A := A_G$). Note that such an η' exists in $\Omega((c-1)^{-1} - c^{-1}) \in \Omega(n^{-2})$. Therefore, WMQS is NP-hard (with respect to n and $\langle \eta' \rangle$) even when $1/\eta'$ is restricted to being in $O(\text{poly}(n))$, which we call *strong* NP-hardness (see [53]).

The second link Gurvits establishes by noting that, via a change of variables $y_i \to x_i^2$,

$$\max_{y \in \Delta_n} y^T Ay = \max_{x \in \mathbf{R}^n, ||x||_2 = 1} \sum_{i,j=1}^{n} A_{ij} x_i^2 x_j^2, \tag{54}$$

and

$$\sum_{i,j=1}^{n} A_{ij} x_i^2 x_j^2 = \sum_{i,j=1}^{n} (\sqrt{A_{ij}} x_i x_j)^2 = 2 \sum_{1 \leq i < j \leq n} (\sqrt{A_{ij}} x_i x_j)^2 = \sum_{1 \leq i < j \leq n} (x^T B^{ij} x)^2, \tag{55}$$

where B^{ij}, for all $1 \leq i < j \leq n$, is the matrix with $\sqrt{A_{ij}}$ in positions (i, j) and (j, i), and zeros elsewhere (note there are $n(n-1)/2$ matrices B^{ij}). Thus RSDF is strongly NP-hard (with respect to l and $\langle \eta \rangle$) in the regime $k \geq l(l-1)/2$, because we can make some of the blocks $B_{i'}$ zero-blocks (the rest of the instance-transformation is $(\zeta, \eta) := (\zeta', \eta')$).

The third link is established in [51], where Gurvits shows that, for

$$B := \begin{pmatrix} 0 & B_1 & \cdots & B_{M-1} \\ B_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ B_{M-1} & 0 & \cdots & 0 \end{pmatrix}, \tag{56}$$

[o] Thanks to Etienne de Klerk at University of Waterloo for pointing me to this theorem.

[p] A_G has a 1 in position (i, j) whenever (i, j) is an edge of G, and otherwise has a 0 (A_G has just zeros on the diagonal).

where the zeros are $N \times N$ blocks of 0 and the B_i are real symmetric $N \times N$ matrices, the following holds:

$$\max_{\sigma \in \mathcal{S}_{M,N}} \mathrm{tr}(B\sigma) = \max_{x \in \mathbf{R}^N, ||x||_2=1} \sum_{i'=1}^{M-1} (x^T B_{i'} x)^2. \tag{57}$$

It follows that WVAL($\mathcal{S}_{M,N}$) is strongly NP-hard (with respect to N and $\langle\epsilon\rangle$) in the regime $M \geq N(N-1)/2+1$ (again, the rest of the instance-transformation is trivial: $(\gamma, \epsilon) := (\zeta, \eta)$). But suppose we had an oracle for WVAL$(\mathcal{S}_{M,N})_{N \leq M \leq N(N-1)/2}$ and wanted to solve the instance of CLIQUE. Then, by setting $M := N := n(n-1)/2+1$ and making each $B_{i'}$ block ($i' = 1, \ldots, N-1$) zeros but for the upper left $n \times n$ submatrix (into which we put B^{ij}), we have that

$$\max_{x \in \mathbf{R}^N, ||x||_2=1} \sum_{i'=1}^{M-1} (x^T B_{i'} x)^2 = \max_{x \in \mathbf{R}^n, ||x||_2=1} \sum_{1 \leq i < j \leq n} (x^T B^{ij} x)^2. \tag{58}$$

Thus WVAL($\mathcal{S}_{M,N}$) is also strongly NP-hard (with respect to N and $\langle\epsilon\rangle$) in the regime $2 \leq N \leq M$.

The last link in the reduction is more correctly split up into two links:

$$\mathrm{WVAL}(\mathcal{S}_{M,N}) \leq_{\mathrm{K}} \mathrm{WVIOL}(\mathcal{S}_{M,N}) \leq_{\mathrm{T}} \mathrm{WMEM}(\mathcal{S}_{M,N}), \tag{59}$$

where the following definition applies:

Definition 14 (Weak violation problem for K (WVIOL(K))) *Given a rational vector $c \in \mathbf{R}^n$, a rational number γ, and rational $\epsilon > 0$, either*

- *assert $c^T x \leq \gamma + \epsilon$ for all $x \in K$, or*

- *find a vector $y \in S(K, \epsilon)$ with $c^T y \geq \gamma - \epsilon$.*

It is clear that WVIOL($\mathcal{S}_{M,N}$) is also strongly NP-hard. But the Turing-reduction from WVIOL($\mathcal{S}_{M,N}$) to WMEM($\mathcal{S}_{M,N}$) is highly nontrivial in that the only proof of this reduction, appearing in Theorem 4.3.2 of [50], requires the shallow-cut ellipsoid method. The accuracy parameters for the WMEM($\mathcal{S}_{M,N}$)-oracle queries in this reduction only have exponentially small lower bounds. Thus the problem remains:

Problem 2 *Is* WMEM($\mathcal{S}_{M,N}$) *tractable when $1/\delta$ is in $O(poly(M, N))$?*

Let us consider the following problem, which is more difficult than the weak membership problem because it asks for the normal vector to a separating hyperplane in the case where the given point is not inside the convex set:

Definition 15 (Weak separation problem for K (WSEP(K))) *Given a rational vector $p \in \mathbf{R}^n$ and rational $\delta > 0$, either*

- *assert* $p \in S(K, \delta)$, *or*
- *find a rational vector* $c \in \mathbf{R}^n$ *with* $||c||_\infty = 1$ *such that* $c^T x < c^T p + \delta$ *for every* $x \in K$.

Note that WSEP($\mathcal{S}_{M,N}$) asks either to assert that the given density matrix is almost separable, or to find an approximate entanglement witness. A Turing reduction from WVIOL($\mathcal{S}_{M,N}$) to WSEP($\mathcal{S}_{M,N}$) (one of which appears in Theorem 4.2.2 of [50]), is much more straightforward and does not require the ellipsoid method – any cutting-plane algorithm for the weak nonemptiness problem[q] relative to a weak separation oracle suffices. Applying the analytic-center algorithm of Atkinson and Vaidya [64] gives a Turing-reduction that only needs to make polynomially-accurate WSEP($\mathcal{S}_{M,N}$)-queries:

Fact 5 WSEP($\mathcal{S}_{M,N}$) *is strongly NP-hard (w.r.t.* N *and* $\langle\delta\rangle$*) in the regime* $2 \le N \le M$.

2.2.6 Possibility of a Karp Reduction

To date, every decision problem (except for QSEP) that is known to be in NPC_T is also known to be in NPC_K [65].[r] While it is strongly suspected that Karp and Turing reductions are inequivalent within NP, it would be surprising if QSEP, or some other formulation of the quantum separability problem,[s] is the first example that proves this inequivalence:

Problem 3 *Is* QSEP *in* NPC_K*?*

One reason to believe that a Turing reduction is necessary to prove the NP-hardness of the quantum separability problem is that a proof (see Section 2.2.5) seems to require a reduction from WVAL($\mathcal{S}_{M,N}$) to WMEM($\mathcal{S}_{M,N}$); in turn, this reduction seems to require the shallow-cut ellipsoid method (a Turing reduction). It is a long-standing open problem as to whether the reduction from WVAL($\mathcal{S}_{M,N}$) to WMEM($\mathcal{S}_{M,N}$) can be done differently. However, as the NP-hardness of WMEM($\mathcal{S}_{M,N}$) is a relatively recent result, there may be an altogether different proof of it that does not require a reduction from WVAL($\mathcal{S}_{M,N}$) to WMEM($\mathcal{S}_{M,N}$).

Note that, because of Fact 3, a negative answer to Problem 3 implies that P $\neq$ NP. Note also that a direct reduction from some $\Pi' \in \text{NPC}_\text{K}$ to QSEP (or some other formulation) would depend heavily on the precise definition of QSEP rather than the true spirit of the quantum separability problem captured by WMEM($\mathcal{S}_{M,N}$). Thus, if the answer to Problem 3 is positive, it might be easier to look for a Karp-reduction from some $\Pi \in \text{NPC}_\text{K}$ to WMEM($\mathcal{S}_{M,N}$).

[q] The weak nonemptiness problem for K is merely to find a point in $S(K, \epsilon)$ or assert that $S(K, -\epsilon)$ is empty.

[r] By "known to be in NPC_T", I mean that the language corresponding to the decision problem can be defined and shown to be Turing-NP-complete, independent of any unproven assumptions. See [66] for languages that are suspected to be Turing-but-not-Karp-NP-complete, whose existence depends on unproven assumptions about NP.

[s] By "formulation of the quantum separability problem", I mean an NP-contained approximate formulation that tends to EXACT QSEP as the accuracy parameters of the problem tend to zero.

3 Survey and complexity analysis of algorithms for the quantum separability problem

For the survey, I concentrate on proposed algorithms that solve an approximate formulation of the quantum separability problem and have (currently known) asymptotic analytic bounds on their running times. For this reason, the SDP relaxation algorithm of Eisert et al. is not mentioned here (see Section 1.2.2); though, I do not mean to suggest that in practice it could not outperform the following algorithms on typical instances. As well, I do not analyze the complexity of the naive implementation of every necessary and sufficient criterion for separability, as it is presumed that this would yield algorithms of higher complexity than the following algorithms. For an exhaustive list of all such criteria, see the book by Bengtsson and Zyczkowski [67].

I give complexity estimates for several of the algorithms surveyed. The main purpose below is to get a time-complexity estimate in terms of the parameters M, N, and δ, where δ is the accuracy parameter in WMEM($\mathcal{S}_{M,N}$). The running-time estimates are based on the number of elementary arithmetic operations and do not attempt to deal with computer round-off error; I do not give estimates on the total amount of machine precision required. Instead, where rounding is necessary in order to avoid exponential blow-up of the representation of numbers during the computation, I assume that the working precision[t] can be set large enough that the overall effect of the round-off error on the final answer is either much smaller than δ or no larger than, say, $\delta/2$ (so that doubling δ takes care of the error due to round-off).

3.1 Naive algorithm and δ-nets

The naive algorithm for any problem in NP consists of a search through all potential succinct certificates that the given problem instance is a "yes"-instance. Thus QSEP immediately gives an algorithm for the quantum separability problem. Hulpke and Bruß [57] have demonstrated another hypothetical guess-and-check procedure that does not involve the probabilities p_i. They noticed that, given the vectors $\{[|\psi_i^{\rm A}\rangle], [|\psi_i^{\rm B}\rangle]\}_{i=1}^{M^2N^2}$, one can check that

$$\{[|\psi_i^{\rm A}\rangle][\langle\psi_i^{\rm A}|] \otimes [|\psi_i^{\rm B}\rangle][\langle\psi_i^{\rm B}|]\}_{i=1}^{M^2N^2} \text{ is affinely independent; and} \tag{60}$$

$$[\rho] \in \operatorname{conv}\{[|\psi_i^{\rm A}\rangle][\langle\psi_i^{\rm A}|] \otimes [|\psi_i^{\rm B}\rangle][\langle\psi_i^{\rm B}|]\}_{i=1}^{M^2N^2} \tag{61}$$

in polynomially many arithmetic operations (and they give an algorithm for the separability problem based on this observation). We can, in principle, reformulate QSEP to incorporate the ideas of Hulpke and Bruß in order to get a better naive algorithm. The reader is referred to [68] for details (and for how our approach differs from theirs – essentially, their algorithm solves a more exact formulation of the separability problem); we quote the asymptotic running-time estimate of $(MN/\delta)^{O(M^3N^2+M^2N^3)}$.

QSEP can be further reformulated to avoid searching through *all* p-bit-precise pure states by using the concept of a net on (or covering of) the unit sphere. Let $\mathbf{S}_M$ be the Euclidean unit sphere in $\mathbf{C}^M$. In principle, we can use a *Euclidean δ-net of* $\mathbf{S}_M$, which is a minimal set of points $\mathcal{N}_\delta^M := \{|x_i\rangle\}_{i=1}^{|\mathcal{N}_\delta^M|} \subset \mathbf{S}_M$ such that for any $|x\rangle \in \mathbf{S}_M$ there exists $|x_i\rangle \in \mathcal{N}_\delta^M$

[t] "Working precision" is defined as the number of significant digits the computer uses to represent numbers during the computation.

such that $|||x\rangle - |x_i\rangle||_2 \leq \delta$. The optimal size of a δ-net on the real sphere is known to be no larger than $(1+2/\delta)^M$ [69], thus we can take $|\mathcal{N}_\delta^M| \leq (1+2/\delta)^{2M}$.[u] Assuming the availability of asymptotically optimal $\mathcal{N}_\delta^M$ for all M and δ (where the real elements in each $|x_i\rangle$ have p bits of precision), the complexity of the naive algorithm for separability is reduced to $(2/\delta)^{O(M^3N^2+M^2N^3)}$, which simply corresponds to the number of M^2N^2-subsets of $\mathcal{N}_\delta^M \times \mathcal{N}_\delta^N$. We will assume availability, or *advice*, of δ-nets for the complexity estimates of several of the following algorithms.

3.2 Bounded search for symmetric extensions

In Section 1.2.1, we considered two tests – one that searches for symmetric extensions of ρ, and a stronger one that searches for PPT symmetric extensions. Now I show that recent results can put an upper bound on the number k of copies of subsystem A when solving an approximate formulation of the separability problem. The bound only assumes symmetric extensions, *not* PPT symmetric extensions, so it is possible that a better bound may be found for the stronger test (Problem 4).

If a symmetric state $\varrho \in \mathcal{D}((\mathbf{C}^d)^{\otimes n})$ has a symmetric extension to $\mathcal{D}((\mathbf{C}^d)^{\otimes(n+m)})$ for all $m > 0$, then it is called *(infinitely) exchangeable*. The quantum de Finetti theorem (see [2] and references therein) says that the infinitely exchangeable state ϱ is separable. Recalling the terminology of Section 1.2.1, it is also possible to derive that, for $\rho \in \mathcal{D}(\mathbf{C}^M \otimes \mathbf{C}^N)$, if there exists a symmetric extension of ρ to k copies of subsystem A for all $k > 0$, then $\rho \in \mathcal{S}_{M,N}$. This is the result that proves that Doherty et al.'s hierarchy of tests is complete: if ρ is entangled, then the SDP at some level k_0 of the hierarchy will not be feasible (i.e. will not find a symmetric extension of ρ to k_0 copies of subsystem A).

It seems reasonable that, if we are only interested in whether ρ is δ-close to $\mathcal{S}_{M,N}$, we should not need to check for extensions of ρ to k copies of subsystem A for k larger than some bound $\bar{k} = \bar{k}(M, N, \delta)$. In fact, we can use results of Christandl et al. [3] to compute just such a $\bar{k}$.[v] We require the following theorem:

Theorem 2 ([3]) *Suppose $\rho \in \mathcal{D}_{M,N}$ and there exists a Bose-symmetric extension ρ' of ρ to $k \geq 2$ copies of subsystem* A*, i.e. $(I \otimes P)\rho' = \rho'$ for all $k!$ permutations P of the k copies of subsystem* A*. Then*

$$tr|\rho - \sigma| \leq \frac{4M}{k}, \tag{62}$$

for some $\sigma \in \mathcal{S}_{M,N}$.

Note that the result uses the *trace distance*, $\mathrm{tr}|X - Y|$, between two operators X and Y. Let us assume we are solving the weak membership formulation of the quantum separability problem with respect to the trace distance, and with accuracy parameter δ. Then, setting $\delta = 4M/k$, we get the following upper bound for k:

[u] Recall that the Euclidean distance between two vectors in $\mathbf{C}^M$ depends only on the real part of their inner product, which behaves exactly like the dot-product of real vectors in $\mathbf{R}^{2M}$.

[v] Thanks to Andrew Doherty for calling my (and Christandl et al.'s!) attention to this; otherwise, I would be deriving a worse bound on k, based on results in [70].

Corollary 1 *To solve* WMEM$(\mathcal{S}_{M,N})$ *(with respect to the trace distance) with accuracy parameter δ by searching for symmetric extensions (as described in Section 1.2.1), it suffices to look for symmetric extensions to*

$$\bar{k} := \lceil 4M/\delta \rceil \tag{63}$$

copies of subsystem A.

To estimate the total complexity of the algorithm, note that

$$\begin{aligned} d_{S_k} &= \binom{M+k-1}{k} \approx \binom{M+k}{k} = \frac{(M+k)!}{k!M!} & (64)\\ &\approx \frac{1}{\sqrt{2\pi}} \frac{(M+k)^{M+k}}{k^k M^M} \left(\frac{1}{k} + \frac{1}{M}\right)^{1/2}, & (65)\\ & & (66) \end{aligned}$$

where in the last line we used Stirling's approximation $n! \approx n^n \sqrt{2\pi n}/e^n$. Substituting $\bar{k} \approx 4M/\delta$ for k, we get

$$\begin{aligned} \left(\frac{1}{\bar{k}} + \frac{1}{M}\right)^{-1/2} d_{S_{\bar{k}}} &\approx \frac{1}{\sqrt{2\pi}} \frac{(M + 4M/\delta)^{M+\bar{k}}}{(4M/\delta)^{\bar{k}} M^M} = \frac{1}{\sqrt{2\pi}} \frac{(1+4/\delta)^{M+\bar{k}}}{(4/\delta)^{\bar{k}}} & (67)\\ &\approx \frac{1}{\sqrt{2\pi}} (4/\delta)^M & (68)\\ d_{S_{\bar{k}}} &\approx \frac{1}{\sqrt{2\pi}} (4/\delta)^M \left(\delta/4M + 1/M\right)^{1/2} & (69)\\ &\approx \frac{1}{\sqrt{2\pi}} (4/\delta)^M \left(1/M\right)^{1/2}. & (70) \end{aligned}$$

Just to solve the first constraint in (7) requires $\sqrt{n}$ (but usually far fewer) iterations of a procedure that requires $O(m^2 n^2)$ arithmetic operations, for $m = ((d_{S_{\bar{k}}})^2 - M^2)N^2$ and $n = (d_{S_{\bar{k}}})^2 N^2$ [2]. That is, the complexity of each iteration is on the order of $(d_{S_{\bar{k}}})^8 \text{poly}(M, N, \log(1/\delta))$.

Problem 4 *Can the upper bound $\bar{k}$ be improved by taking into consideration the PPT constraints in (7)?*

We mention that a larger bound $\bar{k}' \gg \bar{k}$ on k can be derived from a theorem in [70], which also can be used to compute an approximate separable decomposition of ρ in the case where the SDP algorithm finds a symmetric extension of ρ to $\bar{k}'$ copies of subsystem A.

3.3 Entanglement-witness search via global optimization

Recall that an *entanglement witness (for ρ)* is defined to be any operator $A \in \mathbf{H}_{M,N}$ such that $\text{tr}(A\sigma) < \text{tr}(A\rho)$ for all $\sigma \in \mathcal{S}_{M,N}$ and some $\rho \in \mathcal{E}_{M,N}$; we say that "$A$ detects ρ". Since every $\rho \in \mathcal{E}_{M,N}$ has an entanglement witness that detects it [22], one way to solve the quantum separability problem is to exhaustively (but not naively!) search for an entanglement witness for the given ρ. We mention that the dual of the SDP in the symmetric-extension search algorithm can be used to find an (approximate) entanglement witness for ρ (when the SDP is infeasible) [2].

3.3.1 Large SDP method

Pérez-Garcia and Cirac [71] note that the following SDP effectively searches for an approximate entanglement witness $-A$ for ρ:

$$\begin{aligned} \text{minimize} \quad & \mathrm{tr}(A\rho) && (71)\\ \text{subject to:} \quad & \langle x_i|A|x_i\rangle \geq 0,\ \text{for all } |x_i\rangle \in \mathcal{N}_\delta^M, \text{ and } \mathrm{tr}(A) = 1. && (72) \end{aligned}$$

Define the following convex hull:

$$C := \mathrm{conv}\{|x_i\rangle\langle x_i| \otimes |b\rangle\langle b| : |x_i\rangle \in \mathcal{N}_\delta^M, |b\rangle \in \mathbf{C}^N\}. \tag{73}$$

If the minimum is negative, then $-A$ is an approximate entanglement witness for ρ because there is a hyperplane with normal $-A$ that separates ρ from C (otherwise ρ is in C and is thus in $\mathcal{S}_{M,N}$). This is justified because for any $\rho \in \mathcal{S}_{M,N}$ there exists a $\sigma \in C$ such that $||\rho-\sigma||_1 \leq 2\delta$, as we now verify. First, note that if $|||x\rangle-|y\rangle||_2 \leq \delta < 1$, then $\mathrm{Re}\langle x|y\rangle \geq 1-\delta^2/2$ (since $|||x\rangle - |y\rangle||_2^2 = 2 - 2\mathrm{Re}\langle x|y\rangle$) and thus

$$\begin{aligned} |||x\rangle\langle x| - |y\rangle\langle y|||_1 &= 2\sqrt{1-|\langle x|y\rangle|^2} \qquad \text{(see [55], p. 415)} && (74)\\ &\leq 2\sqrt{1-(\mathrm{Re}\langle x|y\rangle)^2} && (75)\\ &\leq 2\sqrt{1-(1-\delta^2/2)^2} && (76)\\ &= 2\delta\sqrt{1-\delta^2/4} && (77)\\ &< 2\delta. && (78) \end{aligned}$$

If $\rho = \sum_j \lambda_j |u_j\rangle\langle u_j| \otimes |v_j\rangle\langle v_j|$, for $\lambda_j \geq 0$ and $\sum_j \lambda_j = 1$, then choosing $|x_{i_j}\rangle \in \mathcal{N}_\delta^M$ such that $|||x_{i_j}\rangle - |u_j\rangle||_2 \leq \delta$ makes $\sigma := \sum_j \lambda_j |x_{i_j}\rangle\langle x_{i_j}| \otimes |v_j\rangle\langle v_j|$ in C with $||\rho - \sigma||_1 \leq 2\delta$.

The size (up to a constant factor) of the constraint of the SDP is $n = |\mathcal{N}_\delta^M|N$ (and the number of real variables to parametrize A is $m = M^2N^2 - 1$), thus the complexity of one iteration of the SDP is of the order $|\mathcal{N}_\delta^M|^2\mathrm{poly}(M, N, \log(1/\delta))$ (assuming $\mathcal{N}_\delta^M$ is available).

This approach is a discretization of Brandão and Vianna's robust semidefinite program (see Section 1.2.4), which is

$$\begin{aligned} \text{minimize} \quad & \mathrm{tr}(A\rho) && (79)\\ \text{subject to:} \quad & x^\dagger Ax \geq 0,\ \text{for all } x \in \mathbf{C}^M, \text{ and } \mathrm{tr}(A) = 1. && (80) \end{aligned}$$

(Note that, combined with Gurvits' NP-hardness result [51], this demonstrates that robust semidefinite programs are, in general, NP-hard.) Essentially, Pérez-Garcia and Cirac have removed the robustness by using a δ-net, which clarifies the complexity of the approach for deterministically solving WMEM($\mathcal{S}_{M,N}$).

3.3.2 Interior-point cutting-plane algorithm with global optimization subroutine

The algorithms in [4, 5] solve WMEM($\mathcal{S}_{M,N}$) by solving WSEP($\mathcal{S}_{M,N}$) using a subroutine for WOPT($\mathcal{S}_{M,N}$):

Definition 16 (Weak optimization problem for K (WOPT(K))) *Given a rational vector $c \in \mathbf{R}^n$ and rational $\epsilon > 0$, either*

- *find a rational vector $y \in \mathbf{R}^n$ such that $y \in S(K, \epsilon)$ and $c^T x \leq c^T y + \epsilon$ for every $x \in K$; or*

- *assert that $S(K, -\epsilon)$ is empty.*[w]

Clearly, using a subroutine for $\mathrm{WOPT}(\mathcal{S}_{M,N})$ allows one to test whether a Hermitian operator A approximately detects ρ. The algorithms effectively perform a binary search through the space of all entanglement witnesses. For example, the algorithm in [4] searches through the space $\mathcal{W} := \{A \in \mathbf{H}_{M,N} : \mathrm{tr}(A) = 0, \mathrm{tr}(A) \leq 1\}$ of all normalized entanglement witnesses by iterating the following:

(i) Let A be an approximate center (interior point) of the current search space (which is initialized to $\mathcal{W} \cap \{x \in \mathbf{H}_{M,N} : \mathrm{tr}(\rho x) \geq 0\}$, but subsequently gets approximately halved in each iteration, in step (iv) below).
(ii) Set $A := A/||A||_2$ and give $(A, \epsilon := \delta/5)$ to $\mathrm{WOPT}(\mathcal{S}_{M,N})$ subroutine, which outputs σ_A.
(iii) If A approximately detects ρ, then return A;
(iv) otherwise, use σ_A to generate a cutting plane which approximately halves the current search space (cuts it through A and the origin). If current search space is too small to contain a hyperplane that separates ρ from $S(\mathcal{S}_{M,N}, \delta)$, then return "$\rho \in S(\mathcal{S}_{M,N}, \delta)$".

The number of arithmetic operations required by the algorithm described in [4] is

$$O((T + M^6 N^6 \log(1/\delta)) M^2 N^2 \log^2(M^2 N^2/\delta)), \tag{81}$$

where T is the cost of one call to the $\mathrm{WOPT}(\mathcal{S}_{M,N})$ subroutine (see [68] for details).

Now consider the complexity of computing an instance (A, ϵ) of $\mathrm{WOPT}(\mathcal{S}_{M,N})$, $||A||_2 = 1$. For each $x_i \in \mathcal{N}_\delta^M$, we compute $|j_i\rangle := \mathrm{argmax}_{|j\rangle} |\langle x_i|\langle j|A|x_i\rangle|j\rangle|$ via eigenvector analysis of $\langle x_i|A|x_i\rangle$ (which is Hermitian).[x] Let $\tilde{i}$ denote the index i of an element $|x_i\rangle$ of $\mathcal{N}_\delta^M$ that maximizes $|\langle x_i|\langle j_i|A|x_i\rangle|j_i\rangle|$. Then $|x_{\tilde{i}}\rangle|j_{\tilde{i}}\rangle$ may be taken as a solution to $\mathrm{WOPT}(\mathcal{S}_{M,N})$ because

$$|\langle x_{\tilde{i}}|\langle j_{\tilde{i}}|A|x_{\tilde{i}}\rangle|j_{\tilde{i}}\rangle - \max_{|\alpha\rangle|\beta\rangle} \langle\alpha|\langle\beta|A|\alpha\rangle|\beta\rangle| \leq 2\delta, \tag{82}$$

[w]For ϵ we consider, this will never be the case for us, as we only consider $\mathrm{WOPT}(\mathcal{S}_{M,N})$ and $\mathcal{S}_{M,N}$ is far from empty.

[x]Thanks to David Pérez-Garcia for suggesting this method.

as we now verify. Let $|a\rangle|b\rangle := \mathrm{argmax}_{|\alpha\rangle|\beta\rangle}\langle\alpha|\langle\beta|A|\alpha\rangle|\beta\rangle$ and let i^* denote the index i of an element $|x_i\rangle$ of $\mathcal{N}_\delta^M$ such that $|||x_i\rangle - |a\rangle||_2 \leq \delta$. Writing $|yb\rangle$ for $|y\rangle|b\rangle$ for any $|y\rangle$,

$$\begin{aligned}
& |\langle x_{i^*}b|A|x_{i^*}b\rangle - \langle ab|A|ab\rangle| && (83)\\
= \;& |\langle x_{i^*}b|A|x_{i^*}b\rangle - \langle ab|A|x_{i^*}b\rangle + \langle ab|A|x_{i^*}b\rangle - \langle ab|A|ab\rangle| && (84)\\
= \;& |||x_{i^*}\rangle - |a\rangle||_2 \left| \frac{\langle x_{i^*}| - \langle a|}{|||x_{i^*}\rangle - |a\rangle||_2}\langle b|A|x_{i^*}b\rangle + \langle ab|A\frac{|x_{i^*}\rangle - |a\rangle}{|||x_{i^*}\rangle - |a\rangle||_2}|b\rangle \right| && (85)\\
\leq \;& 2\delta \max_{|c\rangle,|d\rangle\in\mathbf{C}^M} |\langle c|\langle b|A|d\rangle|b\rangle| && (86)\\
\leq \;& 2\delta \max_{|c'\rangle,|d'\rangle\in\mathbf{C}^M\otimes\mathbf{C}^N} |\langle c'|A|d'\rangle| && (87)\\
= \;& 2\delta \max\{\sqrt{\lambda} : \lambda \text{ an eigenvalue of } A^\dagger A\} \qquad \text{(see [72], p. 312)} && (88)\\
\leq \;& 2\delta\sqrt{\sum_i \lambda_i(A^\dagger A)} \qquad \text{(where } \lambda_i(X) \text{ denotes eigenvalues of } X\text{)} && (89)\\
= \;& 2\delta||A||_2 \qquad \text{(since } A \text{ is normal, see [72], p. 316)} && (90)\\
= \;& 2\delta. && (91)
\end{aligned}$$

The inequality (82) follows from noting

$$\langle x_{i^*}|\langle b|A|x_{i^*}\rangle|b\rangle \leq \langle x_{i^*}|\langle j_{i^*}|A|x_{i^*}\rangle|j_{i^*}\rangle \leq \langle x_{\tilde{i}}|\langle j_{\tilde{i}}|A|x_{\tilde{i}}\rangle|j_{\tilde{i}}\rangle \leq \langle a|\langle b|A|a\rangle|b\rangle. \qquad (92)$$

Therefore, the complexity of the whole algorithm is on the order of $|\mathcal{N}_\delta^M|\mathrm{poly}(M, N, \log(1/\delta))$ (assuming $\mathcal{N}_\delta^M$ is available).

3.4 Other algorithms

We mention two other algorithms, whose running times cannot be easily compared to that of the above algorithms.

3.4.1 Cross-norm criterion via linear programming

Rudolph [73] derived a simple characterization of separable states in terms of a computationally complex operator norm $||\cdot||_\gamma$. For a finite-dimensional vector space V, let $\mathcal{T}(V)$ be the class of all linear operators on V. The norm is defined on $\mathcal{T}(\mathbf{C}^M)\otimes\mathcal{T}(\mathbf{C}^N)$ as

$$||t||_\gamma := \inf\{\sum_{i=1}^k ||u_i||_1||v_i||_1 : \; t = \sum_{i=1}^k u_i \otimes v_i\}, \qquad (93)$$

where the infimum is taken over all decompositions of t into finite summations of elementary tensors, and $||X||_1 := \mathrm{tr}(\sqrt{X^\dagger X})$. Rudolph showed that $||\rho||_\gamma \leq 1$ if and only if $||\rho||_\gamma = 1$, and that a state ρ is separable if and only if $||\rho||_\gamma = 1$.

Pérez-Garcia [74] showed that approximately computing this norm can be reduced to a linear program (which is a special case of a semidefinite program): $\min\{c^T x : \quad Ax = b, x \geq 0\}$, where $A \in \mathbf{R}^{n\times m}$, $b \in \mathbf{R}^n$, $c \in \mathbf{R}^m$, and x is a vector of m real variables; here, $x \geq 0$ means that all entries in the vector are nonnegative. An LP can be solved in $O(m^3 L')$ arithmetic operations, where L' is the length of the binary encoding of the LP [75]. The linear program has on the order of M^2N^2 variables and $|\mathcal{N}_{1/k}^M|^2|\mathcal{N}_{1/k}^N|^2$ constraints, where k is an integer that determines the relative error[y] $(k/(k-1))^4 - 1$ on the computation of the norm. Thus

[y] The *relative error* of an approximation $\tilde{x}$ of x is defined as $|x - \tilde{x}|/x$.

the complexity of the whole algorithm is on the order of $|\mathcal{N}_{1/k}^{M}|^2|\mathcal{N}_{1/k}^{N}|^2\mathrm{poly}(M,N,\log(1/\delta))$ (assuming availability of Euclidean $(1/k)$-nets).

Suppose $||\rho||_\gamma$ is found to be no greater than $1+\eta$. Then, we would like to use η to upper-bound the distance, with respect to either trace or Euclidean norm, from ρ to $\mathcal{S}_{M,N}$. Unfortunately, we do not know how to do this. This drawback, along with the fact that the error on the computed norm is relative as opposed to absolute, does not allow this algorithm to be easily compared to the other algorithms we consider.

3.4.2 Fixed-point iterative method

Zapatrin [76] suggests an iterative method that solves the separability problem.[z] He defines the function $\Phi : \mathbf{H}_{M,N} \to \mathbf{H}_{M,N}$:

$$\Phi(X) := X + \lambda\left(\rho - \int\int e^{\langle\psi^{\mathrm{A}}|\otimes\langle\psi^{\mathrm{B}}|X|\psi^{\mathrm{A}}\rangle\otimes|\psi^{\mathrm{B}}\rangle}|\psi^{\mathrm{A}}\rangle\langle\psi^{\mathrm{A}}|\otimes|\psi^{\mathrm{B}}\rangle\langle\psi^{\mathrm{B}}|d\mathbf{S}_M d\mathbf{S}_N\right), \tag{96}$$

where $\mathbf{S}_M$ and $\mathbf{S}_N$ are the complex origin-centred unit spheres (containing, respectively, $|\psi^{\mathrm{A}}\rangle$ and $|\psi^{\mathrm{B}}\rangle$), and λ is a constant dependent on the derivative (with respect to X) of the quantity in parentheses (λ is chosen so that Φ is a contraction mapping). In earlier work [77, 78, 79], Zapatrin proves that any state σ in the interior $\mathcal{S}_{M,N}^{\circ}$ of $\mathcal{S}_{M,N}$ may be expressed

$$\sigma = \int\int e^{\langle\psi^{\mathrm{A}}|\otimes\langle\psi^{\mathrm{B}}|X_\sigma|\psi^{\mathrm{A}}\rangle\otimes|\psi^{\mathrm{B}}\rangle}|\psi^{\mathrm{A}}\rangle\langle\psi^{\mathrm{A}}|\otimes|\psi^{\mathrm{B}}\rangle\langle\psi^{\mathrm{B}}|d\mathbf{S}_M d\mathbf{S}_N \in \mathcal{S}_{M,N}, \tag{97}$$

for some Hermitian X_σ. Thus the function Φ has a fixed point $X_\rho = \Phi(X_\rho)$ if and only if $\rho \in \mathcal{S}_{M,N}^{\circ}$. When $\rho \in \mathcal{S}_{M,N}^{\circ}$, then a neighbourhood (containing 0) in the domain of Φ can be found where iterating $X_{i+1} := \Phi(X_i)$, starting at $X_0 := 0$, will produce a sequence $(X_i)_i$ that converges to X_ρ when $\rho \in \mathcal{S}_{M,N}^{\circ}$, but diverges otherwise.

Each evaluation of $\Phi(X)$ requires $M^2N^2/2 + MN$ integrations of the form

$$\int\int e^{\langle\psi^{\mathrm{A}}|\otimes\langle\psi^{\mathrm{B}}|X|\psi^{\mathrm{A}}\rangle\otimes|\psi^{\mathrm{B}}\rangle}\langle\mathbf{e}_j^{\mathrm{A}}|\psi^{\mathrm{A}}\rangle\langle\mathbf{e}_{j'}^{\mathrm{B}}|\psi^{\mathrm{B}}\rangle\langle\psi^{\mathrm{A}}|\mathbf{e}_k^{\mathrm{A}}\rangle\langle\psi^{\mathrm{B}}|\mathbf{e}_{k'}^{\mathrm{B}}\rangle d\mathbf{S}_M d\mathbf{S}_N, \tag{98}$$

where $\{\mathbf{e}_j^{\mathrm{A}}\}_j$ and $\{\mathbf{e}_k^{\mathrm{B}}\}_k$ are the standard bases for $\mathbf{C}^M$ and $\mathbf{C}^N$. However, the off-diagonal ($j \neq k$, $j' \neq k'$) integrals have a complex integrand so are each really two real integrals; thus the total number of real integrations is M^2N^2. Let Ξ_δ represent the number of pure states at which the integrand needs to be evaluated in order to perform each real numerical integration, in order to solve the overall separability problem with accuracy parameter δ. Zapatrin shows that the approximate number of iterations required is upper-bounded by

[z] Facts about iterative methods: First, the basic Newton-Raphson method in one variable. Suppose ξ is a zero of a function $f : \mathbf{R} \to \mathbf{R}$ and that f is twice differentiable in a neighbourhood $U(\xi)$ of ξ. Then the Taylor expansion of f about $x_0 \in U(\xi)$ gives

$$\begin{aligned} 0 = f(\xi) &= f(x_0) + (\xi - x_0)f'(x_0) + \cdots \qquad (94) \\ &= f(x_0) + (\tilde{\xi} - x_0)f'(x_0), \qquad (95) \end{aligned}$$

where $\tilde{\xi} = x_0 - f(x_0)/f'(x_0)$ is an approximation of ξ. Repeating the process, with a truncated Taylor expansion of f about $\tilde{\xi}$, gives a different approximation $\tilde{\tilde{\xi}} = \tilde{\xi} - f(\tilde{\xi})/f'(\tilde{\xi})$. This suggests the iterative method $x_{i+1} = \Phi(x_i)$, for $\Phi(x) := x - f(x)/f'(x)$. If $f'(\xi) \neq 0$, the sequence $(x_i)_i$ converges to ξ if x_0 is sufficiently close to ξ. More generally, if $\Phi(x) : \mathbf{R}^n \to \mathbf{R}^n$ is a contractive mapping on $B(x_0, r)$, then the sequence $(x_0, \Phi(x_0), \Phi(\Phi(x_0)), \ldots)$ converges to the unique fixed point in $B(x_0, r)$ (as long as $\Phi(x_0) \in B(x_0, r)$) [27].

$2N(N+1)L(\log(1/\delta), \log(N))$, where L is a bilinear function of its arguments. The complexity of the entire algorithm is roughly $\Xi_\delta \mathrm{poly}(M, N, \log(1/\delta))$ (ignoring $\log(N)$ factors). We can use nets on $\mathcal{S}_M$ and $\mathcal{S}_N$ to estimate the complexity of Ξ_δ. It is clear that the numerical integration is more complex than solving WOPT($\mathcal{S}_{M,N}$); at the very least, it needs to sample points in $\mathcal{S}_N$ as well as $\mathcal{S}_M$. Thus, I make the reasonable presumption that $\Xi_\delta \geq |\mathcal{N}_\delta^M||\mathcal{N}_\delta^N|$.

3.5 Complexity comparison of algorithms and practical considerations

The complexity estimates in the survey show that the two best algorithms are the bounded search for symmetric extensions (Section 3.2) and the cutting-plane entanglement-witness search algorithm (Section 3.3.2). The dominant (exponential) factors in the asymptotic complexity estimates are

$$(d_{S_{\bar{k}}})^8 \approx 2^M \times (1/\delta)^{8M} \qquad \text{(symmetric-extensions search)} \tag{99}$$

$$|\mathcal{N}_\delta^M| \approx 2^M \times (1/\delta)^{2M} \qquad \text{(entanglement-witness search).} \tag{100}$$

As a caveat, recall that the estimate for the entanglement-witness search algorithm assumes the advice of asymptotically optimal $\mathcal{N}_\delta^M$, which in principle can be precomputed for the M and δ of interest [80].

The bounded symmetric-extension search algorithm only experiences "exponential slowdown" when k approaches $\bar{k}$. The SDP relaxation algorithm of Section 1.2.2 behaves similarly, in that successive SDP relaxations get larger, while the first SDP relaxation is feasible. Thus, a good strategy for a deterministic WMEM($\mathcal{S}_{M,N}$) solver might be to start with these algorithms (after exhausting all the other efficient one-sided tests), and proceed until the SDPs get infeasibly large; then, switch to the entanglement-witness search algorithm, whose complexity bottleneck is the WOPT($\mathcal{S}_{M,N}$) subroutine, which has constant worst-case complexity throughout the execution of the algorithm, but whose task – essentially, searching the domain of the function $f(|\alpha\rangle, |\beta\rangle) := \langle\alpha|\langle\beta|A|\alpha\rangle|\beta\rangle$ – can be parallelized. Interestingly, the subroutine need not find a certified optimum of f until its final execution, and even then only in the case where the algorithm will output $\rho \in S(\mathcal{S}_{M,N}, \delta)$ [4]; thus, comparing the outputs of executions of a local optimum finder seeded at a few random points in the domain may suffice for at least some of the WOPT($\mathcal{S}_{M,N}$) calls. Finally, instead of using δ-nets, the subroutine should benefit from more-sophisticated, continuous global optimization methods (which may utilize calculus to eliminate large chunks of the domain of f) such as the semidefinite programming relaxation method of Lasserre [35], Lipschitz optimization [81], and Hansen's global optimization algorithm using interval analysis [82].

Acknowledgements

Thanks to Matthias Christandl, Roger Colbeck, Anuj Dawar, Andrew Doherty, Daniel Gottesman, Alastair Kay, Michele Mosca, Renato Renner, and Tom Stace for helpful discussions. Special thanks to David Pérez-Garcia for his help with Section 3.3. This work was supported by the CESG (UK), NSERC (Canada), ORS (UK), RESQ (EU grant IST-2001-37559), and EPSRC.

References

[1] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Distinguishing separable and entangled states. *Phys. Rev. Lett.*, 88:187904, 2002.

[2] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Complete family of separability criteria. *Phys. Rev. A*, 69:022308, 2004.

[3] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-half quantum de finetti theorems, 2006. quant-ph/0602130.

[4] L. M. Ioannou, B. C. Travaglione, D. C. Cheung, and A. K. Ekert. Improved algorithm for quantum separability and entanglement detection. *Phys. Rev. A*, 70:060303(R), 2004.

[5] L. M. Ioannou and B. C. Travaglione. Quantum separability and entanglement detection via entanglement-witness search and global optimization. *Phys. Rev. A*, 73:052314, 2006.

[6] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232:333, 1997.

[7] Dagmar Bruß. Characterizing entanglement. *J. Math. Phys.*, 43:4237, 2002.

[8] B. M. Terhal. Detecting quantum entanglement. *Journal Theoretical Computer Science*, 287(1):313–335, 2002.

[9] A. Sen De, U. Sen, M. Lewenstein, and A. Sanpera. The separability versus entanglement problem, 2005. quant-ph/0508032.

[10] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, 1996.

[11] M. Horodecki and P. Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Phys. Rev. A*, 59:4206, 1999.

[12] R. Horodecki, P. Horodecki, and M. Horodecki. Quantum α-entropy inequalities: independent condition for local realism? *Phys. Lett. A*, 210:377–381, 1996.

[13] M. Nielsen and J. Kempe. Separable states are more disordered globally than locally. *Phys. Rev. Lett.*, 86:5184–7, 2001.

[14] O. Rudolph. Further results on the cross norm criterion for separability, 2002. quant-ph/0202121.

[15] K. Chen and L.-A. Wu. A matrix realignment method for recognizing entanglement. *Quant. Inf. Comp.*, 3:193, 2003.

[16] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Separability of mixed quantum states: linear contractions approach, 2002. quant-ph/0206008.

[17] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for NMR quantum computing. *Phys. Rev. Lett.*, 83:1054, 1999.

[18] L. Gurvits and H. Barnum. Largest separable balls around the maximally mixed bipartite quantum state. *Phys. Rev. A*, 66:062311, 2002.

[19] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Phys.Rev. A*, 58:883, 1998.

[20] G. Vidal and R. Tarrach. Robustness of entanglement. *Phys. Rev. A*, 59:141, 1999.

[21] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein. Separability in $2 \times n$ composite quantum systems. *Phys. Rev. A*, 61:062302, 2000.

[22] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1–8, 1996.

[23] P. Horodecki, M. Lewenstein, G. Vidal, and I. Cirac. Operational criterion and constructive checks for the separabilty of low-rank density matrices. *Phys. Rev. A*, 62:032310, 2000.

[24] S. Albeverio, Shao-Ming Fei, and Debashish Goswami. Separability of rank two quantum states. *Phys. Lett. A*, 286:91–96, 2001.

[25] J. H. Wilkinson and C. Reinsch. *Linear Algebra, Handbook for Automatic Computation Vol. II.* Springer-Verlag, Berlin, 1971.

[26] Gene H. Golub and Charles F. van Loan. *Matrix Computations.* The Johns Hopkins University Press, Baltimore, 1996.

[27] J. Stoer and R. Bulirsch. *Introduction to numerical analysis.* Springer-Verlag, New York, 2002.

[28] J. H. Wilkinson. Global convergence of tridiagonal QR algorithm with origin shifts. *Lin. Alg. Appl.*, 1:409–420, 1968.

[29] M. Lewenstein and A. Sanpera. Separability and entanglement of composite quantum systems. *Phys. Rev. Lett.*, 80:2261, 1998.

[30] R. T. Thew, K. Nemoto, A. G. White, and W. J. Munro. Qudit quantum-state tomography. *Phys. Rev. A*, 66:012303, 2002.

[31] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.

[32] M. Fannes, J. T. Lewis, and A. Verbeure. Symmetric states of composite systems. *Lett. Math. Phys.*, 15:255, 1988.

[33] C. M. Caves, C. A. Fuchs, and R. Schack. Unknown quantum states: The quantum de finetti representation. *J. Math. Phys.*, 43:4537, 2002.

[34] Jens Eisert, Philipp Hyllus, Otfried Gühne, and Marcos Curty. Complete hierarchies of efficient approximations to problems in entanglement theory. *Phys. Rev. A*, 70:062317, 2004.

[35] Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3):796–817, 2001.

[36] Didier Henrion and Jean-Bernard Lasserre. GloptiPoly: Global optimization over polynomials with Matlab and SeDuMi. *ACM Transactions on Mathematical Software*, 29(2): 165–194, 2003.

[37] V. Vedral, M. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Phys. Rev. Lett.*, 78:2275–2279, 1997.

[38] Matthias Christandl. *Bipartite Entanglement: A Cryptographic point of view.* PhD thesis, University of Cambridge, 2005.

[39] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglementand quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, 1996.

[40] Armin Uhlmann. Optimizing entropy relative to a channel or a subalgebra. *OPEN SYS.AND INF.DYN.*, 5:209, 1998. URL `http://arxiv.org/abs/quant-ph/9701014`.

[41] Fernando G. S. L. Brandão and Reinaldo O. Vianna. Robust semidefinite programming approach to the separability problem. *Phys. Rev. A*, 70:062309(R), 2004.

[42] Fernando G. S. L. Brandão and Reinaldo O. Vianna. Separable multipartite mixed states: Operational asymptotically necessary and sufficient conditions. *Phys. Rev. Lett.*, 93:220503, 2004.

[43] Hugo J. Woerdeman. Checking $2\times m$ quantum separability via semidefinite programming. *Phys. Rev. A*, 67:010303(R), 2003.

[44] P. Horodecki and A. Ekert. Method for direct detection of quantum entanglement. *Phys. Rev. Lett.*, 89:127902, 2002.

[45] W. C. Myrvold. The decision problem for entanglement. In R. S. Cohen, M. Horne, and J. Stachel, editors, *Potentiality, entanglement and passion-at-a-distance*, pages 177–190. Kluwer Academic Publishers, 1997.

[46] K. Weihrauch. *Computability.* Springer-Verlag, Berlin, 1987.

[47] A. Seidenberg. A new decision method for elementary algebra. *Annals of Mathematics*, 60(2):365–374, 1954.

[48] Alfred Tarski. A decision method for elementary algebra and geometry. Technical report, University of California, Berkeley, 1951.

[49] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of the ACM*, 43(6):1002–1045, 1996.

[50] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization.* Springer-Verlag, Berlin, 1988. ISBN 038713624x.

[51] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the thirty-fifth ACM symposium on Theory of computing*, pages 10–19, New York, 2003. ACM Press.

[52] Kristopher Luttmer. The complexity of separability testing. Master's thesis, University of Calgary, 2005.

[53] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the theory of NP-completeness.* W.H. Freeman and Company, New York, 1979.

[54] C. H. Papadimitriou, editor. *Computational complexity.* Addison Wesley Longman, Reading, Massachusetts, 1994.

[55] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[56] R. Ladner, N. Lynch, and A. Selman. Comparison of polynomial-time reducibilities. *Theoretical Computer Science*, 1:103–123, 1975.

[57] Florian Hulpke and Dagmar Bruß. A two-way algorithm for the entanglement problem. *J. Phys. A: Math. Gen.*, 38:5573, 2005.

[58] Otfried Gühne and Norbert Lütkenhaus. Nonlinear entanglement witnesses. *Phys. Rev. Lett.*, 96:170502, 2006.

[59] S. Aaronson. Private communication. 2005.

[60] A. Ben-Tal and A. Nemirovskii. Robust convex optimization. *Mathematics of Operational Research*, 23(4):769–805, 1998.

[61] L. Gurvits. Private communication. 2006.

[62] L. Gurvits and H. Barnum. Better bound on the exponent of the radius of the multipartite separable ball. *Phys. Rev. A*, 72:032322, 2005.

[63] T. S. Motzkin and E. G. Straus. Maxima for graphs and a new proof of a theorem of turán. *Canadian J. Math.*, 17:533–540, 1965.

[64] David S. Atkinson and Pravin M. Vaidya. A cutting plane algorithm for convex programming that uses analytic centers. *Mathematical Programming*, 69:1–43, 1995.

[65] A. Pavan and Alan L. Selman. Separation of NP-completeness notions. *SIAM J. Comput.*, 31(3):906–918, 2001.

[66] A. Pavan. Comparison of reductions and completeness notions. *SIGACT News*, 40, 2003.

[67] Ingemar Bengtsson and Karol Zyczkowski. *Geometry of separable states.* Cambridge University Press, Cambridge, 2006.

[68] L. M. Ioannou. Computing finite-dimensional bipartite quantum separability, 2005. PhD thesis, available at http://arXiv.org/abs/cs/0504110.

[69] G. Pisier, editor. *The volume of convex bodies and Banach space geometry.* Cambridge University Press, Cambridge, 1989.

[70] Robert König and Renato Renner. A de Finetti representation for finite symmetric quantum states. *J. Math. Phys.*, 46:122102, 2005.

[71] D. Pérez-Garcia and I. Cirac. Private communication. 2006.

[72] Roger A. Horn and Charles R. Johnson. *Matrix Analysis.* Cambridge University Press, Cambridge, 1985.

[73] Oliver Rudolph. A separability criterion for density operators. *J. Phys. A*, 33:3951–3955, 2000.

[74] David Pérez-Garcia. Deciding sepability with a fixed error. *Phys. Lett. A*, 330:149–154, 2004.

[75] Y. Ye. *Interior Point Algorithms: Theory and Analysis.* John Wiley and Sons, Inc., New York, 1997.

[76] Romàn R. Zapatrin. An asymptotical separability criterion for bipartite density operators, 2005. quant-ph/0504169.

[77] Romàn R. Zapatrin. A note on continuous ensemble expansions of quantum states, 2004. quant-ph/0403105.

[78] Romàn R. Zapatrin. Continuous optimal ensembles i: A geometrical characterization of robustly separable quantum states, 2005. quant-ph/0503173.

[79] Romàn R. Zapatrin. Continuous optimal ensembles ii: Reducing the separability condition to numerical equations, 2005. quant-ph/0504034.

[80] R. H. Hardin, N. J. A. Sloane, and W. D. Smith. *Spherical Codes.* In preparation, see http://www.research.att.com/∼njas/coverings/index.html.

[81] R. Horst and P. Pardalos, editors. *Handbook of Global Optimization.* Kluwer Academic Publishers, Dordrecht, 1995.

[82] E. Hansen. *Global Optimization Using Interval Analysis.* Marcel Dekker Incorporated, Boston, 1992. ISBN 0824786963.